Université de Montréal

L'audit de sécurité et la protection des organisations

par

Sylvain Mignault

École de criminologie

Faculté des Arts et des Sciences

Mémoire présenté à la Faculté des études supérieures

en vue de l'obtention du grade de

Maître ès sciences (M.Sc.)

en criminologie

Janvier 2009

Université de Montréal

Faculté des études supérieures

Ce mémoire intitulé :

L'audit de sécurité et la protection des organisations

présenté par :

Sylvain Mignault

a été évalué par un jury composé des personnes suivantes :

Stéphane Leman-Langlois, président-rapporteur

Maurice Cusson, directeur de recherche

Frédéric Lemieux, membre du jury

Mémoire accepté le : _____

RÉSUMÉ

Il peut être difficile pour un néophyte de mettre le doigt sur les problèmes de sécurité d'une organisation, et encore pire, de trouver des solutions appropriées. Cette tâche n'est pas toujours plus facile pour les experts qui ont à travailler pour des organisations qui ont des problèmes complexes et qui ont à choisir parmi un choix de solutions grandissant. Le gestionnaire se doit d'agencer intelligemment des mesures en choisissant parmi le matériel de sécurité, l'embauche de personnel, l'achat d'équipement électronique, l'implantation de procédures ou l'innovation dans le but de trouver des solutions nouvelles. L'audit est un outil qui aide les experts à effectuer ce travail.

Nous définissons l'audit, ou le relevé de sécurité, comme étant un examen méthodique d'une organisation ou d'un site visant à identifier ses risques, ses vulnérabilités et les faiblesses de ses protections existantes ainsi qu'à statuer sur son niveau de sécurité et à recommander des solutions aux problèmes identifiés. Cet examen permet de recueillir beaucoup de données concernant l'organisation. Celles-ci sont par la suite analysées pour trouver des solutions adaptées et efficaces pour régler les problèmes de sécurité rencontrés.

Il y a deux types de données qui sont collectées lors d'un audit. Il y a celles qui sont quantitatives avec lesquelles il est possible de faire des analyses statistiques. Essentiellement, l'expert les trouve en consultant l'historique des incidents d'une organisation, les résultats des tests qui peuvent avoir été effectués sur les équipements de sécurité en place ou encore à l'aide des outils informatiques disponibles. Malheureusement, les données statistiques ne sont pas toujours accessibles. Les données qualitatives constituent le deuxième type de données. Elles sont collectées en allant rencontrer les personnes clés d'une organisation, en consultant des documents ou en observant les lieux. Idéalement, l'expert collecte le maximum de données qualitatives et quantitatives. Cela lui permet d'effectuer de bonnes analyses avant de faire ses recommandations finales.

L'objectif général de cette recherche est d'analyser les audits de sécurité effectués par les acteurs chargés de la sécurité et vérifier s'ils utilisent la littérature spécialisée ainsi que les théories développées en criminologie. Les experts de la région de Montréal réalisent des audits de sécurité et nous voulons vérifier comment ils procèdent pour réaliser ces projets pour les organisations. Leur façon de faire ressemble à celle développée par les experts anglophones et nous expliquerons d'où provient cette ressemblance. Nous avons retenu cinq étapes à la réalisation d'un projet d'audit qui sont les suivantes : 1) La rencontre préliminaire 2) la préparation 3) la cueillette des données 4) l'analyse des données et 5) la rédaction d'un rapport. Ces étapes seront expliquées et critiquées dans ce mémoire.

Pour rencontrer notre objectif général, nous avons opté pour une recherche effectuée à l'aide de données qualitatives. Seize experts ont participé à cette recherche, nous avons fait onze entretiens non-directifs, étudié six cas, effectué deux séances d'observations et finalement nous avons assisté à une conférence donnée par les membres de l'ASIS International (chapitre Montréal).

Dans cette recherche, nous allons aussi faire un lien entre les audits réalisés par les experts et l'analyse qui est faite en criminologie. L'analyse criminologique jumelée à la façon de faire pragmatique des experts peut constituer un apport dans ce domaine. Les criminologues ont développé des méthodes efficaces pour étudier le crime et pour analyser les problèmes. Utiliser ces méthodes dans le cadre d'un audit améliorerait l'analyse des données qui est souvent négligée par les experts. Joindre le savoir-faire des experts de la sécurité privée à celui des criminologues permettrait de cibler les problèmes et de leur attribuer des solutions praticables.

Un exemple de guide de sécurité[1] est fourni dans ce mémoire. Il s'agit d'une grille de questions qui est utilisée par l'ensemble des experts que nous avons rencontrés. Cette grille permet d'étudier les éléments de la sécurité d'une organisation et d'éviter les oublies. Pour plusieurs, il s'agit d'un outil très utile, voire indispensable.

[1] Les anglophones utilisent le terme 'security survey'.

MOTS CLÉS : Audit de sécurité, guide de sécurité, sécurité privée, analyse des risques

ABSTRACT

It might be difficult for a beginner to make the security problems of an organization apparent, and even harder to find the appropriate solutions. This task is not always easy for the experts who work for organizations dealing with complex problems to decide between many solutions. The manager has to hire people, to purchase electronic equipment, to set up procedures, or to break new ground to find new solutions. The security survey is a useful tool in helping the experts to do their work.

We define the security survey as a methodical examination of an organization or of a site aiming to identify its risks, its vulnerabilities and its existing protection weaknesses, to find its security level and to recommend solutions to the identified problems. The exam allows for the collecting of a large amount of data concerning the organization. Then, they are analyzed to eventually find adapted and efficient solutions to resolve the security problems coming across.

There are two types of data collected during a security survey. There is the quantitative data from which it is possible to make statistic analysis. Essentially, the expert finds it by consulting the historic incidents of an organization the results of tests made on security equipment in place or with the help of available informatics tools. Unfortunately, the statistic data are not always available. The qualitative data constitutes the second type of data. It is collected when meeting the people of an organization, consulting documents or observing places. The expert collects as much quantitative and qualitative data as possible because it helps to make a better analysis before giving final recommendations.

The general objective of this research is to analyze and to describe the security survey realized by the actors in charge of the security and verify if they use the criminological analysis and the experts pragmatic methods. The experts from the Montreal area use this tool and we will show how they use it. Their methods are similar to the ones developed by the American experts and we explain where this similarity comes from. To realize a security survey, we use five steps: 1) A preliminary meeting, 2)

Preparation, 3) Information research, 4) Analysis and 5) writing of a report. These steps are explained and criticized in this thesis.

To reach our general goal, we opted for a research made of qualitative data. In total, we met 16 experts, had eleven meetings, six cases were studied, two sessions of observation, and finally, we assisted at a conference given by members of ASIS International (Montreal chapter).

We also compare the methods of the specialists we met with the criminological analysis. The criminological analysis mixed at the experts pragmatic methods is a contribution in the domain. The criminologists developed efficient methods to study crime or to analysis the problems. To use these methods in an audit substantially improves the analysis of information which is often left out by experts. To combine the private security experts' knowledge to the criminologists' would allowed.

An example of the security survey is provided in this thesis. A security survey is a questions scale used by all of the experts we met. This scale allows us to study security elements of an organization without leaving any out. For many it is a useful and essential tool.

KEY WORDS : Security survey, private security, risk analysis

TABLE DES MATIÈRES

RÉSUMÉ ..... **iii**
ABSTRACT ..... **vi**
TABLE DES MATIÈRES ..... **viii**
TABLEAU ET GUIDE DE SÉCURITÉ ..... **xii**
REMERCIEMENTS ..... **xiii**

INTRODUCTION **1**

1. RECENSION DES ÉCRITS **5**

1.1 L'audit de sécurité : mesure de contrôle social 5
1.2 L'audit de sécurité et son effet dissuasif 8
1.3 L'offre et la demande d'audit de sécurité 11
1.4 L'audit de sécurité dans une perspective d'analyse et de gestion des risques 13
1.5 La réalisation d'un audit de sécurité 17

1.5.1 La visite préliminaire 17
1.5.2 La préparation 19
1.5.3 La cueillette des données 21
1.5.4 L'analyse des données 23
1.5.5 La rédaction du rapport 25

1.6 L'après audit 28

2. PROBLÉMATIQUE **32**

Question de recherche 32

3. MÉTHODOLOGIE **33**

3.1 Objectifs de la recherche 33
3.2 Délimitation de l'objet d'étude 34
3.3 Sélection du corpus empirique 35

3.3.1 Constitution du corpus 35
3.3.2 Saturation empirique des données 37
3.3.3 Diversification des données 37

3.4 Méthodes de cueillette des données 38

3.4.1 Les entretiens semi-directifs 39
3.4.2 L'analyse de cas 40
3.4.3 L'observation participante 41
3.4.4 Conférence donnée par ASIS International (chapitre de Montréal) 41

3.5 Méthode d'analyse des données 42

4. LA RÉALISATION D'UN AUDIT DE SÉCURITÉ 45

4.1 American Society for Industrial Security (ASIS Int.) 45

4.1.1 Certifications offertes par ASIS Int. 46
4.1.2 Littérature et publications 46
4.1.3 Activités ASIS Int. 48
4.1.4 Impact de l'organisation ASIS Int. sur nos données 48

4.2 Terminologie 49

4.2.1 Inspection de sécurité 52
4.2.2 Étude de sécurité 53
4.2.3 Visite de sécurité 53
4.2.4 Audit de sécurité 54
4.2.5 Confusion au niveau de la terminologie 56
4.2.6 Sécurité ou sûreté ? 58

4.3 Audit : projet en développement 59
4.4 Audit de sécurité dans un contexte général 59
4.5 Audit : projet circonscrit ou exercice continu 61
4.6 La demande des audits de sécurité 63

4.6.1 Raisons qui expliquent la demande 63
4.6.2 Problématiques 64
4.6.3 Investissement en sécurité 64
Le cas Ralphy *65*
4.6.4 L'audit de sécurité et le programme de sécurité 67

4.7 La préparation 70

4.7.1 S'informer au sujet de l'organisation 70
4.7.2 La finesse de l'expert 70
4.7.3 Rencontre avec la personne-ressource 71
4.7.4 Les raisons qui limitent le mandat 73
4.7.5 Cibler les priorités 75
4.7.6 Visite sommaire des lieux 76

4.8 Guide de sécurité (liste de contrôle) 76

4.8.1 Guide adapté à l'organisation 77
4.8.2 Évolution de l'outil 78
4.8.3 Format du guide 78
4.8.4 L'expert derrière l'outil 79

4.8.5 Exemple de guide de sécurité 80
4.8.6 Le guide d'inspection et la prévention situationnelle 84

4.9 Terrain 84

4.9.1 Informations recherchées 85
4.9.2 Types de données recueillies 86
4.9.3 Méthode qualitative 87

Rencontre avec les employés 88
Observation 89
Analyse documentaire 90
Tests de la sécurité 90
Outils de travail 90

4.9.4 Méthode quantitative 91
4.9.5 Importance de la démarche terrain et de la collecte des données 93

4.10 Analyse des données 93

4.10.1 Application de concepts criminologiques 93
4.10.2 Audit de sécurité et l'analyse des problèmes en criminologie 94
4.10.3 L'approche pragmatique des experts en sécurité privée 96
4.10.4 Analyse des risques 98
4.10.5 Analyse coût/bénéfice 98
4.10.6 Niveau d'analyse 99

4.11 Rapport 99

4.11.1 Le rapport : efforts pour les experts 100
4.11.2 Information qui s'y trouve 100
4.11.3 Présentation du rapport 101
4.11.4 Qualité du rapport 102

4.12 Recommandations 102

4.12.1 Types de solutions 102
4.12.2 Mesures innovatrices 103
4.12.3 Solutions pour une sécurité parfaite ? 104
4.12.4 La rentabilisation de la sécurité 104
4.12.5 Pouvoir décisionnel 105
4.12.6 Surprise des gestionnaires 106
4.12.7 Solutions alternatives 106
4.12.8 Planification dans le temps 107

4.13 Fin du projet d'audit 107

4.14 L'audit et la recherche en criminologie 107

4.15 Les experts, la littérature spécialisée et les concepts criminologiques 108

5. CAS ENTREPÔT FROST (OBSERVATION) 110

5.1 Présentation des experts 110
5.2 Entrepôt Frost 110
5.3 Travail effectué par les experts 112

5.3.1 Première visite 112
5.3.2 Deuxième visite 112
5.3.3 Autres visites 114
5.3.4 Rapport 114

5.4 Présentation du rapport et fin du projet 116

CONCLUSION 117

BIBLIOGRAPHIE 122

TABLEAU ET GUIDE DE SÉCURITÉ

Tableau 1 : Terminologie utilisée par les experts 51

Guide de sécurité (liste de contrôle)..... 80

REMERCIEMENTS

Merci aux professeurs et aux superviseurs de stage qui ont cru en mon potentiel et qui m'ont encouragé à poursuivre mes différents projets. Merci à mes professeurs au collégial et à Robert Trépanier qui m'ont convaincu d'entreprendre mes études universitaires. Merci à Hélène Raza, à Sylvie Archambault et à Maurice Cusson de m'avoir encouragé à compléter le programme de maîtrise à l'École de criminologie.

Un merci spécial pour Maurice Cusson pour m'avoir offert un projet emballant ainsi que la chance de rédiger le chapitre 26 du *Traité de Sécurité intérieure* (2007). En tant que directeur, vous avez su m'apporter votre aide aux moments où j'en avais besoin et me transmettre vos connaissances. C'est une grande chance d'avoir pu travailler avec vous.

Merci à tous les experts d'avoir pris le temps de me rencontrer. Sans vous, il ne m'aurait pas été possible de compléter ce mémoire. Une mention spéciale est due à Stéphane Veilleux (membre influent de l'ASIS International et expert pour Pharmascience) pour m'avoir aidé tout au long de mes travaux.

Merci à mes amis et amies qui m'ont connu un peu plus effacé à certains moments tout au long du programme de maîtrise. Je n'ai pas été en mesure de les voir aussi souvent que je l'aurais espéré. Merci pour votre support et votre intérêt vis-à-vis mon sujet d'étude.

Finalement, je tiens à remercier profondément ma famille qui a toujours été là pour moi. Sans votre soutien, vos encouragements et votre présence, il m'aurait été beaucoup plus difficile de me rendre là où je suis aujourd'hui. Je vous dois beaucoup. Merci Valérie, Liliane et Norbert.

INTRODUCTION

Avant de planifier un dispositif de sécurité, le professionnel commence par analyser l'organisation que nous lui demandons de sécuriser. L'audit de sécurité (en anglais : *security survey* ; nous utiliserons aussi l'expression *relevé de sécurité*) aide à effectuer cette analyse, permet de statuer sur le niveau de sécurité d'une organisation, de constater les faiblesses ainsi que les excès de sécurité et à trouver des solutions intéressantes aux problèmes de sécurité existants ou à venir (Roper, 1997 : 13; Johnson, 2005 : 333). Cette démarche est utile pour déterminer les actions à accomplir pour atteindre un niveau de protection adéquat (Mombroisse 1968 : 13; Kingsbury 1973 : 6). Nous définissons l'audit ou le relevé de sécurité comme étant un examen méthodique d'une organisation ou d'un site qui vise à identifier ses risques, ses vulnérabilités et les faiblesses de ses protections existantes, à statuer sur son niveau de sécurité et à recommander des solutions aux problèmes identifiés. Dans le cadre de ce relevé, le professionnel se rend sur les lieux pour examiner l'organisation. Cet examen porte sur le milieu environnant, le périmètre de sécurité, les infrastructures, les actifs, le système de sécurité, les opérations, le personnel, les incidents passés, les procédures et les politiques ayant un impact sur la sécurité. Il identifie les éléments susceptibles d'affecter la sécurité, les évalue et procède à des recommandations le cas échéant.

La sécurité privée a connu une croissance importante durant les trois dernières décennies (Brodeur 2003 ; Cunningham 1990). Les effectifs et les budgets rattachés au secteur de la sécurité privée ont respectivement presque doublé et quintuplé selon les projections effectuées par Cunningham et ses collègues (1990). Cette expansion s'est réalisée dans plusieurs pays, dont le Canada et les États-Unis. Ce développement est expliqué par plusieurs facteurs (Cunningham 1990 : 236; Piché 2000 : 29-31). L'un de ces facteurs est le fait que le secteur privé offre aux gens une protection supplémentaire à celle offerte par le secteur public (Brodeur 2003 : 295-308). Ce niveau de protection, ne pouvant pas être entièrement fourni par les acteurs publics, est offert par les entreprises privées de sécurité. En effet, ces entreprises offrent aux clients plusieurs biens et services pouvant combler l'écart entre le niveau de sécurité

qu'ils demandent et ce qui est offert par les services publics (Institut des hautes études de la sécurité intérieure (IHESI) 1991 : 139; Collins, Ricks et Van Meter 2000; AQIS 2004 : 11).

Les façons de faire et de penser la sécurité dans le secteur privé se modifient. Il y a moins de gardes qui patrouillent les sites et plus de gestionnaires qui ont la tâche de gérer la sécurité des organisations (Cunningham, 1990; Cusson, 1998 b : 40; Dégailler, 1998 : 63 et 66). Il y a davantage d'équipements de sécurité qui sont offerts sur le marché et qui sont susceptibles d'être utilisés par les gens pour se protéger des crimes (Brodeur, 2003 ; Cunningham, 1990). Une gamme très diversifiée de produits et services est maintenant offerte sur le marché de la sécurité. Une plus grande place est accordée à la technologie et à l'expertise (Cusson, 1998 : 40-45). Les technologies évoluent très rapidement et elles protègent plus efficacement les organisations lorsqu'elles sont bien utilisées. Elles amènent des défis importants aux gestionnaires qui ont à choisir, installer et utiliser les technologies. Ces défis peuvent devenir un casse-tête pour les gestionnaires (Leman-Langlois et Dupuis 2007 : 437).

Cette croissance et ces changements amènent des nouveaux défis pour les organisations qui doivent faire des choix éclairés pour mieux se protéger. Ces défis sont plus faciles à relever pour les petites entreprises, mais ils peuvent s'avérer plus difficiles pour les organisations complexes, en croissance ou de grandes tailles (National Crime Prevention Institute (NCPI) 1986 : 24; Berger 1999 : 15; Walsh et coll. 1994, 2-I-5; Fischer et Green 2004 : 129). Le défi est de choisir les équipements utiles, efficaces et efficients. Certains choix d'équipements nécessitent de gros investissements. Pour se protéger, « il ne s'agit pas de déployer à l'aveuglette le matériel et les hommes, mais de miser sur l'intelligence » (Cusson 1998 b : 44). Les équipements sécuritaires doivent être sélectionnés judicieusement et être installés adéquatement pour être efficaces (Cusson, 1998 b : 41).

Pour mieux protéger leurs actifs, les gens sont invités à faire appel à des experts de la sécurité privée (Cusson 1998 : 45). Les organisations peuvent avoir un service de

sécurité interne ou faire appel à une agence de sécurité contractuelle. Ces professionnels ont le mandat de protéger les intérêts des organisations en les conseillant sur ce qui doit être fait en matière de sécurité. Par exemple, il est possible qu'un dirigeant d'entreprise hésite entre l'embauche d'agents de sécurité et l'acquisition de caméras de surveillance. Quels sont les avantages et les inconvénients reliés à ces choix ? Comment intégrer ces mesures de sécurité ? Est-ce qu'elles sont permises par la loi ? Est-ce qu'elles sont vraiment nécessaires ? Quelles sont les alternatives ? Plusieurs questions ressortent lorsqu'il est question d'investir dans des mesures de sécurité. Les experts savent répondre à ces questions et aident les organisations à faire des choix judicieux. Ils ont des outils qui les aident à prendre des décisions éclairées.

La première étape pour sécuriser une organisation est de développer un programme de sécurité. Le relevé de sécurité va aider au développement de ce programme (Momboisse 1968 : 13; Berger 1999 : 17). Les experts auditent les organisations pour déterminer leurs besoins réels. L'audit débouche sur l'appréciation des risques, sur des choix conscients envers ces risques, sur des recommandations visant la gestion des risques et sur une meilleure planification des dispositifs de protection. L'idée de base est de permettre de dessiner et d'implanter un système adapté aux organisations pour gérer et prévenir les problèmes (National Crime Prevention Institute, 1986 : 27). L'audit est un outil qui aide les experts à prendre les meilleures décisions.

L'objectif principal de ce mémoire est d'analyser les audits de sécurité effectués par les acteurs chargés de la sécurité et vérifier s'ils utilisent la littérature spécialisée ainsi que les théories développées en criminologie. Nous cherchons à savoir si cet outil est utilisé par les experts de la région de Montréal et tâchons de comprendre comment et pourquoi ils l'utilisent. Est-ce qu'ils s'inspirent des ouvrages écrits par les experts en sécurité s'étant intéressés à l'audit de sécurité ? Est-ce qu'ils analysent la sécurité en se basant sur les principes de la prévention situationnelle et de la dissuasion ?

Dans la recension des écrits, nous faisons état de la connaissance en lien avec l'audit de sécurité. Ce dernier est mis dans son contexte. Les étapes suggérées pour réaliser un relevé sont expliquées. Nous situons ce projet dans une perspective d'analyse et de gestion des risques. Nous expliquons pourquoi sa réalisation est considérée comme une mesure de contrôle social. Par la suite, nous exposons notre problématique et la méthodologie qui a été utilisée pour réaliser cette recherche.

Dans le premier chapitre d'analyse, nous expliquons les similitudes qu'il y a entre la façon de faire utilisée par les experts d'ici et celles retrouvées dans la littérature. Quelques termes sont définis et expliqués. Nous utilisons nos données pour dresser le portrait le plus fidèle possible des audits qui sont réalisés par les acteurs que nous avons rencontrés. Nous proposons un exemple de guide de sécurité. Un parallèle est fait entre l'expertise criminologique et l'audit de sécurité. Dans le deuxième chapitre d'analyse, un exemple concret d'audit est donné. Nous avons réalisé un audit avec un expert et nous décrivons cette expérience.

1. RECENSION DES ÉCRITS

Nous nous sommes intéressés à deux genres d'ouvrages. Le premier genre est davantage théorique et il s'agit de documents ayant été rédigés par des criminologues s'étant intéressés au contrôle social, à la prévention situationnelle et à la dissuasion. Le deuxième genre englobe les ouvrages spécialisés portant sur l'audit de sécurité (security survey) écrits par les professionnels de la sécurité. Nous y retrouvons différentes 'recettes' fournies par les professionnels qui expliquent la pertinence de réaliser des audits de sécurité et décrivent leurs façons de procéder.

1.1 L'audit de sécurité : mesure de contrôle social

Il y a un parallèle à faire entre l'audit et la théorie du contrôle social. Pour ce faire, nous utilisons la définition présentée par Cusson (2000 : 123) : « entendons par contrôle social (on dit aussi régulation sociale) l'ensemble des moyens mis en œuvre par les membres d'une société dans le but spécifique de contenir ou de faire reculer le nombre et la gravité des délits ». Suite aux recommandations de l'expert, les citoyens et les organisations peuvent mettre en place des mesures afin de réduire ou d'éliminer certaines problématiques. Ils cherchent ainsi à minimiser les risques d'être affecté par une menace ou d'en réduire l'impact le cas échéant.

Cusson (2000 : chapitre 9) distingue trois catégories de contrôle sociaux : les contrôles sociaux informels, la prévention situationnelle et la sanction pénale. Tout au long de notre vie, nous faisons face aux contrôles sociaux informels. Dès notre jeune âge, nous sommes rapidement confrontés à la pression exercée par les pairs et nous sommes incités à respecter les normes et les valeurs véhiculées par le groupe. Cette pression émane des relations que nous entretenons avec les gens de notre entourage (famille, amis, professeurs, collègues de travail). Bien qu'il soit difficile pour une organisation d'avoir une telle influence sur ses employés, il est toujours possible d'avoir un impact à ce niveau. Pensons aux campagnes de sensibilisation, aux programmes éducatifs ou

aux différentes formations offertes aux employés (exemple : formation concernant l'éthique au travail).

Les organisations peuvent aussi compter sur la prévention situationnelle pour protéger leurs actifs (Cusson 2002 : chapitre 2). Étant donné qu'elles ne peuvent pas se fier uniquement sur les contrôles sociaux informels et sur le système pénal pour se protéger des crimes, elles optent aussi pour différents moyens préventifs. « La notion de prévention situationnelle sert à désigner les mesures non-pénales ayant pour but d'empêcher le passage à l'acte en modifiant les circonstances particulières dans lesquelles des délits semblables sont commis ou pourraient l'être » (Cusson, 2000, 128). À ce niveau, il ne s'agit plus de tenter de changer les gens pour les inciter à ne pas perpétrer de crime (Killias 1991 : 288-331). Nous prenons pour acquis que certains individus sont motivés à commettre des infractions et ainsi affecter les actifs d'une organisation. Les moyens qui relèvent de la prévention situationnelle visent à empêcher ces gens de passer aux actes. Ces moyens peuvent avoir comme résultat de rendre le crime moins payant, plus difficile et/ou plus risqué et ainsi encourager l'individu rationnel à ne pas le commettre (Cornish et Clarke, 1986; Felson & Clarke, 1998 : 24-25; Cusson 2005 : 196). Si après avoir effectué un calcul coûts/bénéfices l'individu considère que le crime ne vaut pas la peine d'être commis, alors il y a de bonnes chances qu'il s'abstienne de le perpétrer (Felson & Clarke, 1998). Quelques catégories de moyens ont été répertoriées : la surveillance et les vérifications ; les protections physiques ; les contrôles d'accès ; les contrôles de facilitateurs ; les détournements et les désintéressements (Cusson, 2002). La théorie de la prévention situationnelle est intéressante puisque plusieurs mesures, solutions et recommandations qui émanent des audits de sécurité sont en fait des moyens rattachés à la prévention situationnelle.

Finalement, les organisations peuvent avoir recours à la sanction pénale pour régler un problème criminel. Même si cette sanction peut être utilisée en dernière instance et qu'il est toujours possible d'y recourir, plusieurs organisations préfèrent souvent ne pas faire appel au secteur public pour régler leurs conflits. La réponse publique est

souvent inadaptée aux besoins et aux désirs des entreprises (Cusson 1998 : 31 et 37 ; Blais 1999 ; Biegaj 2000 ; Brodeur 2003 ; Clarke et Eck 2003 : 4 ; Bacher et Gagnon, 2003; Association québécoise des intervenants de la sécurité (AQIS) 2004 : 27-28). Plusieurs raisons sont invoquées par les organisations pour ne pas référer un cas au système pénal : le coût en temps et en argent d'une poursuite devant les tribunaux peut être élevé; les dirigeants préfèrent garder un certain contrôle sur les procédures, contrôle qu'ils perdent en allant devant les tribunaux ; la réprimande imposée par le système pénal n'est pas toujours celle recherchée par les organisations si bien que les gestionnaires préfèrent trouver une solution mieux adaptée ; la peur d'affecter la réputation de l'organisation en dévoilant ses problèmes criminels au public et l'insatisfaction envers le système pénal (Cusson 1998 : 37; Blais 1999). « Malgré tout, persiste l'illusion voulant que la répression des délits contre la propriété relève de la responsabilité de la police et de la justice. Toutefois, on y croit de moins en moins : dans les entreprises et les commerces, pour se protéger contre le vol, on s'en remet à la sécurité privée et à la prévention situationnelle, non au système pénal. » (Cusson, 2005 : 77). L'expert ne doit pas avoir le réflexe de recourir au système public, mais bien voir ce dernier comme une solution parmi toutes les autres (Leman-Langlois 2007 : 367).

Lorsqu'un délit est commis et que l'organisation ne veut pas faire appel à la police, il y a aussi la possibilité de faire sa propre enquête interne et d'imposer une sanction à l'infracteur (AQIS 2004 : 26-27). Dans son mémoire, Blais (1999) parle d'un « système de justice privée infligeant ses propres sanctions ». Un employé fautif peut se voir sanctionné par son employeur qui le congédie, lui refuse une promotion, le soumet à des contrôles ou le rétrograde (Blais 1999; Bacher et Cousineau 1999). Les clients peuvent aussi être sanctionnés par les organisations. Prenons l'exemple d'un client qui est soupçonné de fraude par une institution financière et dont le nom est placé sur une « liste pénalisante » qui l'empêchera d'avoir différents services ou bénéfices par la suite (Bacher et Gagnon 2003 : 100). Il faut porter une attention spéciale aux sanctions qui peuvent être imposées à l'interne. Cette forme de répression

peut comporter un danger à l'endroit des employés et des clients, surtout si elle est faite à leur insu (Ocqueteau 1991 : 89; Bacher et Gagnon 2003 : 100).

La sécurité privée est un allié pour les organisations puisqu'elle propose un éventail de solutions très large qui correspond aux attentes de celles-ci. Contrairement au système public qui priorise les actions répressives et l'intervention sur des crimes contre la personne, les entreprises privées de sécurité offrent des solutions adaptées aux clients et visent principalement à prévenir les incidents et à protéger leurs biens (Bacher et Gagnon 2003 : 94). Comme nous l'avons mentionné, cet éventail de solutions est principalement constitué de mesures rattachées à la prévention situationnelle, mais aussi de contrôles sociaux informels et de différentes sanctions imposées à l'interne. En effectuant des audits de sécurité et en implantant par la suite un certain nombre de mesures préventives, dissuasives et répressives, les gens et les organisations exercent une forme de contrôle social (Cusson 2000 : 123).

1.2 L'audit de sécurité et son effet dissuasif

Qui sont ces personnes prêtes à commettre des délits et à s'attaquer aux actifs d'une organisation ? Beaucoup de gens gravitent autour des organisations. Il y a les employés qui sont affectés aux opérations, les gestionnaires, les contracteurs, les clients et toutes les autres personnes qui circulent librement sur un site ou celles qui n'ont pas accès au site mais qui tentent tout de même de s'y introduire à des fins malintentionnées. Les menaces qui pèsent contre les organisations peuvent provenir de l'intérieur si des gens ayant obtenu la confiance de l'organisation décident de s'attaquer à leur employeur ou à leur client. Les menaces peuvent aussi provenir de l'extérieur si des gens n'ayant pas accès au site parviennent à s'y introduire. La majorité des gens sont honnêtes et nous n'avons pas trop à nous en préoccuper. Par contre et comme l'a démontré Cusson (1981), beaucoup de gens ont déjà commis ou sont encore prêts à commettent des délits mineurs. Étant placée devant une opportunité de commettre une infraction facile à réaliser, peu risquée et somme toute payante, une personne peut être tentée de profiter de cette opportunité et de commettre une

infraction. Il est bon de se rappeler que l'opportunité fait le délinquant (Clarke et Eck 2003 : chapitre 10). Il est important pour une organisation de s'assurer de ne pas placer des personnes qui au départ n'auraient pas commis de délit devant des opportunités alléchantes. La plupart des délits ne sont pas planifiés par les infracteurs et sont toutefois réalisés simplement parce que des opportunités sont offertes à un moment donné.

Bien qu'il soit intéressant de tenir compte des opportunités criminelles, il y a d'autres aspects à prendre en considération pour déterminer si un délit va être commis ou non. Pour certains, il est inconcevable de commettre un délit puisqu'ils se considèrent honnêtes et intègres. Le fait de s'attaquer à une organisation se heurte à leurs convictions et leurs valeurs bien ancrées. D'autres ne passeront pas aux actes puisqu'ils ont peur d'être réprimandés s'ils sont pris. Ils ne verront pas l'avantage de perdre leur réputation ou leur emploi pour des délits qui n'en valent pas la peine.

Une minorité de personnes ne se contentent pas seulement des petits délits faciles à réaliser et cherchent à réussir des coups plus fumants. Elles profiteront certainement des opportunités qui s'offriront à elles, mais elles peuvent aussi les provoquer. Les premiers délits peuvent être réalisés par accident et sans trop de planification. Au fur et à mesure que les infracteurs progressent, ils structurent et planifient davantage leurs actions (Felson 2002 : 39). Les délinquants sont rationnels (Cusson 1981; Felson 2002 : 37). Ils tenteront de s'attaquer aux cibles les moins protégées et tenteront de déployer le minimum d'efforts pour arriver à leurs fins. Beaucoup de délinquants sont à la recherche des plaisirs immédiats et tentent de se soustraire de la peine imminente (Cusson 1981; Felson 2002 : 37). Dans ce contexte, une organisation qui offre davantage d'opportunités criminelles et qui est moins bien protégée risque d'être davantage victimisée que l'organisation qui a sa sécurité à cœur et qui se protège de façon plus adéquate.

L'expert doit diminuer au maximum les brèches qui peuvent être exploitées par les criminels et empêcher qu'il y ait des rencontres entre des délinquants motivés et des

cibles intéressantes, vulnérables et mal protégées et cela en l'absence d'un gardien capable d'empêcher le délit (Felson et Clarke 1998 : 4; Killias 2001 : 292-293; Felson 2002 : 21; Clarke et Eck 2003 : chapitre 9; Cusson 2005 : 100). Il s'agit des trois éléments du crime qui sont presque toujours présents (Felson 2002 : 21). Il suffit donc de supprimer l'un de ces éléments pour empêcher des crimes d'être commis. Des mesures doivent être implantées pour mieux protéger les cibles et les rendre moins intéressantes et moins vulnérables. Par exemple, il est possible de placer un gardien qui empêchera que des délits soient perpétrés. Les gardiens ne se limitent pas seulement aux policiers et aux agents de sécurité (Felson 2002 : 21). Nous sommes tous en quelque sorte des gardiens susceptibles de protéger des cibles et d'empêcher des personnes malintentionnées de passer à l'acte (Cusson 2002 : chapitre 3; Felson 2002 : 21-22). Un concierge qui nettoie un établissement procure une présence suffisante pour empêcher un voleur de commettre un vol. Des employés alertes et sensibles aux visiteurs indésirables peuvent les intercepter et les remettent aux autorités en place. Un violeur à l'approche d'une victime potentielle peut se désister en apercevant un autre piéton au loin. Bref, nous jouons tous à un moment le rôle de gardien.

L'audit et les mesures qui sont implantées par la suite ont certainement un effet dissuasif auprès des personnes qui souhaitent s'attaquer à une organisation. En menant à bien un tel projet, l'organisation démontre aux éventuels infracteurs qu'elle a sa sécurité à cœur. De plus, en implantant des mesures elle rend plus difficile et risquée la perpétration des crimes. En se protégeant plus efficacement contre les crimes, la probabilité de la peine augmente et cela dissuade plusieurs personnes de commettre les délits qu'ils avaient envisagés (Cusson 2000 : 135; Cusson 2005 : 93). À court terme, les délinquants peuvent cesser leurs activités criminelles et analyser les nouveaux risques auxquels ils s'exposent. Certains tenteront à nouveau de s'attaquer à l'organisation et c'est à ce moment que les mesures doivent donner les résultats escomptés afin que les délinquants ne réussissent pas leurs coups en toute impunité.

1.3 L'offre et la demande d'audit de sécurité

Toutes les personnes physiques ou morales ayant suffisamment d'actifs à protéger peuvent demander un audit de sécurité. Il peut s'agir autant d'un particulier qui veut protéger sa propriété que d'une entreprise multinationale qui désire connaître le niveau de sécurité de ses sites. Il est possible pour les citoyens et certains commerçants d'utiliser les guides mis à la disposition par les corps de police sur leur site Internet et de faire eux-mêmes l'audit de leurs actifs (maison, garage, appartement, petit commerce). Plusieurs corps de police à travers le monde offrent des guides et des conseils pour améliorer la sécurité physique. Certains offrent aussi la possibilité aux individus qui en ressentent le besoin d'être assistés par un policier pour les aider dans cette démarche. Bien que cette aide puisse être appréciée, elle ne sera pas suffisante pour les organisations plus complexes qui requièrent des examens plus approfondis et des analyses plus poussées (Berger 1999 : 15; Fisher et Green 2004 : 129). Il peut être plus difficile pour elles d'identifier les risques et de déterminer le niveau de sécurité à atteindre.

Plusieurs raisons peuvent amener les organisations à demander un audit de sécurité. Idéalement, il est réalisé à titre préventif. Étant effectué avant qu'un incident affecte l'organisation, nous mettons en place des mesures qui peuvent empêcher une menace d'exploiter une vulnérabilité. Le client peut aussi demander un audit avant d'investir dans des équipements ou des services de sécurité (Purpura 2002 : 226). Les organisations peuvent être sollicitées par plusieurs entreprises qui offrent différents produits et services de sécurité et il est difficile pour un gestionnaire de décider quelles sont les mesures réellement efficaces. Les recommandations qui suivent l'audit vont l'aider à prendre ce genre de décisions et lui épargner d'investir dans des mesures coûteuses et inutiles proposées par des fournisseurs qui pensent à leur profit avant les intérêts de leurs clients (Broder 2000 : 222-223; Purpura 2002 : 226-227). Trop souvent, l'audit va être demandé après un événement regrettable ou une fois que le client aura constaté un réel problème de sécurité au sein de son organisation. Le client fait alors appel à un expert qui confirmera ou infirmera la présence dudit problème.

Les gens peuvent avoir tendance à surévaluer ou sous-évaluer l'importance de la situation (Leman-Langlois 2007 : 373). D'autres raisons peuvent expliquer la demande d'un audit, notamment le désir de se conformer à une réglementation ou à une norme de sécurité (exemple : C-TPAT).

Les experts peuvent être choisis parmi le personnel du service de sécurité interne ou parmi les consultants externes (Momboisse 1968 : 13; Johnson 2005 : 338-340). Le premier avantage d'un audit réalisé par un service de sécurité interne tient au fait qu'il est effectué par des employés ayant une meilleure connaissance de l'organisation. De plus, puisqu'il s'agit de ses propres employés, l'organisation bénéficie d'une plus grande flexibilité (Gagnon 2006 : 18-19). Il est aussi plus facile de mobiliser les ressources. Ce type d'audit coûte moins cher. Il s'agit d'une expérience enrichissante pour les personnes ayant à réaliser le projet (Johnson 2005 : 339). Par contre, les recommandations peuvent être biaisées (Johnson 2005 : 339). Un employé peut ne pas vouloir relever et exposer les faiblesses de son organisation dans un rapport, surtout si elles concernent sa propre personne, son service de sécurité, ses collègues ou encore pire ses supérieurs. Les employés de l'organisation peuvent aussi exagérer les problèmes et recommander des mesures excessives dans le but d'améliorer leurs conditions de travail (Johnson 2005 : 340).

Les conseillers externes, de leur côté, sont souvent plus qualifiés pour réaliser ces projets et peuvent comparer la sécurité entre les organisations. Effectué par des gens de l'extérieur, l'audit risque d'être plus objectif (Gagnon 2006 : 18-19). Par contre, certains conseillers externes ne sont pas toujours d'une impartialité à toute épreuve (Broder 2000 : 223; Johnson 2005 : 340; Leman-Langlois 2007 : 372). Ils peuvent à la fois offrir des services-conseils, vendre de l'équipement et offrir des services de sécurité (exemples : gardiennage, service d'une patrouille privée pour répondre à des alarmes, etc.). Il est important de travailler d'abord et avant tout dans l'intérêt du client et non pour leur propre intérêt mercantile, soit la vente d'un produit ou d'un service.

Qu'elle travaille à l'interne ou comme consultant externe, la personne qui réalise un audit doit avoir une certaine expérience pour mener à bien un tel projet (Roper, 1997 : 4). Cette expérience peut être acquise avec les années d'expérience, l'éducation, à l'aide de formations ou en étant encadré par d'autres gestionnaires ayant cette expertise.

1.4 L'audit de sécurité dans une perspective d'analyse et de gestion des risques

L'American Society for Industrial Security (ASIS International) définit le mot risque comme étant la possibilité d'une perte pouvant être occasionnée par une menace, un incident ou un évènement (2003 : 5). Il existe deux types de risques, les risques purs et les risques dynamiques (National Crime Prevention Institute (NCPI) : 1986 : 42; Hess et Wrobleski 1992 : 81-82). Les premiers n'engendrent que des pertes et aucun bénéfice (exemples : désastres naturels, crimes). Les risques dynamiques quant à eux peuvent occasionner des pertes, mais aussi des bénéfices. Par exemple, en acceptant les chèques, un commerce peut augmenter ses ventes, mais aussi la probabilité de subir des fraudes (Hess et Wrobleski 1992 : 82). Il ne faut pas toujours voir les risques de façon négative. Pour réaliser leurs opérations, les organisations font face à plusieurs risques et il leur appartient de les identifier, les analyser et les gérer.

Selon la terminologie utilisée par ASIS International, l'analyse des risques est un examen détaillé pour estimer, évaluer et gérer les risques, c'est-à-dire les probabilités d'encourir des pertes, des agressions, ou tout autre évènement regrettable. Cette analyse permet de mieux anticiper les événements indésirables susceptibles d'affecter une organisation et d'évaluer les probabilités qu'ils se produisent, ainsi que les impacts qu'ils auraient sur l'organisation (ASIS International 2003 : 5). En se basant sur cette définition, l'analyse des risques comporte six éléments (le sixième élément se rattache davantage à la gestion des risques).

Premièrement, un inventaire des actifs est effectué dans le but d'identifier ceux qui doivent être protégés. Un niveau d'importance est accordé aux divers actifs afin de

connaître les plus stratégiques pour l'organisation. Durant cet inventaire, il ne faut pas se limiter aux biens meubles et immeubles. Il faut par exemple tenir compte des employés, des fournisseurs, de la clientèle, des tierces personnes qui fréquentent les sites, de la notoriété de l'entreprise, des immeubles et des informations. En somme, les actifs sont généralement constitués de biens, de personnes et d'informations.

Deuxièmement, les menaces qui peuvent affecter les actifs de l'organisation sont identifiées. Pour Broder (2000 : 4), une menace peut être définie comme étant toute chose qui peut affecter une organisation et ses actifs. Il peut s'agir d'une catastrophe naturelle, d'un acte criminel, d'un acte terroriste, d'un désastre, d'un désordre civil, d'une guerre, d'un accident ou d'un conflit d'intérêts (Broder 2000 : 5).

Troisièmement, les faiblesses de l'organisation qui rendent les actifs vulnérables sont évaluées (Broder 2000). Par exemple, il peut être constaté que les employés laissent des documents confidentiels dans des classeurs non verrouillés. En découvrant de telles vulnérabilités, l'expert se demande quels sont les correctifs qui peuvent être apportés. Il porte aussi une attention aux contre-mesures qui sont déjà en place. Il s'interroge sur la pertinence et l'efficacité de ces mesures et détermine si elles doivent demeurer en place, être modifiées ou même supprimées. De plus, il détermine si ces contre-mesures sont bien intégrées dans l'organisation. D'excellents dispositifs de sécurité peuvent s'avérer inefficaces à cause de la négligence ou de l'insouciance des employés. Par exemple, le mot de passe pour accéder à un ordinateur n'empêchera pas une tierce personne de l'utiliser si son propriétaire ne verrouille pas son système avant de quitter son poste de travail.

Quatrièmement, une fois les actifs, les menaces et les vulnérabilités identifiés, l'expert évalue les probabilités que les risques surviennent et en évalue l'impact. Il classe les risques selon qu'ils sont certains, très probables, modérément probables, peu probables ou de probabilité inconnue (Walsh et Healy 1994 : 2-I-11; ASIS International 2003 : 18). Les probabilités peuvent aussi être traduites quantitativement lorsqu'il y a des données pour appuyer l'évaluation (exemples : pourcentage, nombre d'événements

anticipés). Il peut être difficile de se faire une idée sur les probabilités qu'un évènement survienne. Walsh et Healy (1994 : 2-I-5 à 2-I-7) énumèrent une série de facteurs qui peuvent avoir un impact sur la probabilité. Ils sont divisés en 5 catégories. Il y a des facteurs liés à l'environnement physique (poids de l'objet, climat, location), à l'environnement social (distribution de la population, groupe d'âge, revenu), à l'environnement politique (organisation sociale), aux expériences antérieures (incidents passés) et finalement à la façon de faire des criminels. Pour établir les risques qui sont les plus probables et ceux qui le sont moins, ces auteurs proposent de les comparer entre eux et de déterminer les risques qui sont plus vraisemblables que les autres et de faire des catégories (Walsh et Healy 1994 : 2-I-10 à 2-I-11).

Cinquièmement, il classe le niveau de gravité du risque selon qu'il est fatal pour l'organisation, très sérieux, modérément sérieux, peu important ou que la gravité de l'impact n'est pas connue (ASIS International 2003 : 20-21). Si possible, l'impact est chiffré. Pour évaluer la gravité de l'impact sur un bien, il ne tient pas seulement compte de sa simple valeur monétaire. Il considère d'autres coûts comme le coût de remplacement du bien, le coût des mesures qui peuvent être prises temporairement pour remplacer le bien, le coût relié à l'arrêt de la production, la perte monétaire (argent et intérêt), l'éventuelle hausse de la prime d'assurance, la perte de marché (client, contrat, notoriété) et tous les autres coûts (Fisher et Green 2004 : 140).

Le NCPI conseille aussi de tenir compte de la probabilité et de l'impact, mais utilise une terminologie différente pour définir ces concepts. Il recommande de déterminer la perte maximale possible (impact maximal) et par la suite la perte maximale probable (probabilité).

Sixièmement, après avoir attribué une probabilité et un impact pour chacun des risques, l'expert les classifie pour en dégager des recommandations. Il se demande si ces risques seront éliminés, réduits, diffusés, transférés ou acceptés par le client (NCPI 1986 : 48-51; Grose 1987 : 47; Hess et Wrobleski 1992 : 91-92; Purpura 2002 : 335; Johnson, 2005 : 335; Garcia 2006 : 2). Il peut être possible d'éliminer certains risques

bien précis. Par exemple, en congédiant un employé malhonnête, le danger que cette personne puisse voler de l'interne est éliminé. Dans la mesure du possible, les gestionnaires voudront mettre en place des contre-mesures afin d'éliminer un risque dont la probabilité et la gravité sont élevées. Quoiqu'il soit souvent impossible d'éliminer complètement les risques, il est toujours possible de les réduire. Le professionnel réduit un risque en diminuant les probabilités qu'il affecte l'organisation ou en diminuant l'impact sur cette dernière. Par exemple, nous réduisons la probabilité de cambriolage en installant un système d'alarme et nous diminuons l'ampleur d'un éventuel vol puisque le voleur quittera les lieux rapidement s'il déclenche l'alarme. En distribuant un risque, le professionnel cherche à répandre ce dernier. En entreposant des objets de valeur à différents endroits, nous parvenons à distribuer le risque de se faire voler l'ensemble de ces objets. Le transfert de risque se réalise souvent avec l'aide des compagnies d'assurances. Un risque improbable avec un niveau de criticité très sérieux sera sûrement transféré à une compagnie d'assurances. Il est toutefois recommandé de diminuer un risque avant de l'assurer. Le coût d'une police d'assurance peut être très dispendieux, mais il est moindre si le propriétaire met en place des mesures pour protéger ses actifs. Les compagnies d'assurances peuvent aussi exiger que des dispositifs soient mis en place avant d'assurer les biens en question (exemple : antivol sur des voitures luxueuses). Finalement, une organisation accepte un risque lorsqu'elle décide sciemment de ne prendre aucune mesure vis-à-vis ce dernier. Des matrices de décisions peuvent être utilisées pour aider à déterminer quelles seront les mesures à adopter pour chacun des risques (voir matrice proposée par Broder 2000 : 31). Cet outil aide à visualiser les risques et à associer des pistes de solution appropriées.

Il est important de ne pas tenter de trouver de solution avant d'avoir terminé l'analyse complète des risques (NCPI, 1986 : 48). Certaines personnes peuvent être tentées de suggérer des solutions avant même d'avoir fait l'analyse des problèmes de sécurité.

C'est donc en identifiant les actifs, les menaces, les vulnérabilités, les probabilités et les impacts que l'expert est en mesure de faire son analyse des risques (Broder 2000;

Collins, Ricks et Van Meter 2000; Purpura 2002; Sennewald 2003; Fennely 2004; Fisher et Green 2004). L'audit de sécurité est un outil éprouvé qui aide l'analyse et la gestion des risques (Broder, 2000 : 41; Johnson, 2005 : 333). En se rendant sur les lieux d'une organisation, le professionnel recueille plusieurs informations pertinentes et utiles pour les gestionnaires qui auront à gérer les risques.

1.5 La réalisation d'un audit de sécurité

En nous inspirant de la façon de faire de Roper (1997 : ch. 2), Broder (2000 : ch. 7 et 8) et Johnson (2005 : ch. 11), nous proposons cinq grandes étapes pour réaliser un audit de sécurité complet : 1) la visite préliminaire, 2) la préparation, 3) la cueillette des données, 4) l'analyse des données et 5) la rédaction d'un rapport. À l'aide de ces cinq étapes, nous exposons ce que la littérature spécialisée recommande comme façons de faire éprouvées par les spécialistes. Il est à noter que cette littérature est peu théorique et qu'elle est presque entièrement basée sur les pratiques directes des experts. Dans le chapitre 4 de ce mémoire, nous chercherons à vérifier si les pratiques des experts rencontrés au cours de notre recherche se rapprochent de ces cinq étapes.

1.5.1 La visite préliminaire

La première étape, la visite préliminaire, permet de réaliser cinq actions : se renseigner sur l'organisation; négocier le mandat; établir les paramètres de l'audit; encourager le personnel à s'approprier le mandat; se familiariser avec les lieux (Johnson 2005 : 345-346).

L'expert commence par se renseigner sur l'organisation. S'il n'a pas une bonne connaissance de l'organisation, il lui sera difficile de remplir son mandat et de mettre en place des mesures appropriées par la suite (Leman-Langlois et Dupuis 2007 : 440-442). Il recueille un maximum d'informations sur son contexte organisationnel, ses caractéristiques, sa clientèle, son historique, son mandat, sa mission, ses valeurs, sa culture organisationnelle et ses objectifs stratégiques. La première rencontre avec le

demandeur est préparée. Les informations ainsi recueillies serviront aussi lors de la cueillette et l'analyse des données.

Par la suite, l'expert rencontre son supérieur ou son client dans le but de concevoir un mandat clair avec lui. Il faut connaître les raisons qui incitent le demandeur à désirer un audit de sécurité et ses attentes vis-à-vis de la démarche (Roper 1997 : 36). Si c'est l'expert qui propose l'audit, il en expose les raisons et explique ce qu'il implique. Cette rencontre est recommandée afin que les deux parties aient une idée claire du projet dès le départ et pour éviter les malentendus.

Troisièmement, le professionnel profite de cette rencontre pour établir les paramètres de l'audit. Il s'entend avec le demandeur sur les objectifs qui doivent être rencontrés et sur les limites du projet (Johnson 2005 : 346). Qu'est-ce qui sera inspecté et qu'est-ce qui ne le sera pas ? Certains actifs sont plus importants que d'autres pour l'organisation et ils doivent être identifiés. Une liste de ces actifs peut être préparée (Roper 1997 :27). Ils conviennent aussi des moyens et des facilités qui seront mis à la disposition de l'expert. Par exemple, ce dernier peut demander à rencontrer certaines personnes, à avoir accès à des secteurs de l'organisation, à tester des dispositifs ou à lire des documents confidentiels. Le demandeur doit lui fournir les accès et les outils nécessaires à la réalisation de son mandat. Un échéancier est aussi prévu.

Quatrièmement, le professionnel construit le mandat avec le demandeur afin que ce dernier s'y intéresse et qu'il se l'approprie. Ayant participé à la conception du mandat et ayant mis des efforts dans le projet, le demandeur sera plus enclin à coopérer pour le reste du processus. La direction doit appuyer le mandat et les paramètres. Il est beaucoup plus facile de travailler si l'expert a l'appui des gestionnaires et des employés. La tenue du projet doit être annoncée à tous les employés de l'organisation (Roper 1997 : 10). Il faut faire attention à l'approche qui sera adoptée et aux mots qui seront utilisés pour présenter le projet aux employés. L'audit ne doit pas être perçu comme une menace par ces derniers (Roper 1997 : 10 et 17). Il est difficile d'obtenir des informations d'un employé qui est fermé au projet.

Finalement, il se familiarise avec les lieux en faisant un examen rapide de l'organisation (Sennewald 1989 : 47; Gagnon 2006 : 90). Cet examen rapide est surtout nécessaire pour le conseiller externe qui ne connaît pas l'organisation.

1.5.2 La préparation

Avant d'entreprendre la cueillette des données, le professionnel se prépare. Il rassemble les outils nécessaires à la réalisation du mandat (exemples : plans, appareil photo). Il se questionne à savoir si une assistance est nécessaire et se concerte avec d'éventuels collaborateurs (Roper 1997 : 25). Si un problème est identifié dès le départ dans le mandat, il formule des hypothèses pouvant l'expliquer qui seront plus tard mises à l'épreuve (Clarke et Eck 2003 : chapitre 20).

C'est aussi à cette étape qu'il élabore un guide (checklist ou liste de contrôle) servant à objectiver et à structurer la démarche. Ce guide est généralement constitué d'un ensemble de questions portant sur les éléments à inspecter. Il peut s'agir de questions ouvertes et de questions fermées (Broder 2000 : 11). Le défi est de choisir les bonnes questions qui permettront de couvrir tous les éléments à auditer, de dresser un portrait fidèle du niveau de sécurité de l'organisation, de trouver les vulnérabilités de même que les excès de sécurité et de bien documenter les recommandations. Le guide sert d'aide-mémoire pour ne rien oublier d'important.

Il y a des guides spécifiques qui cherchent à examiner des éléments très précis (exemple : système informatique). D'autres guides sont beaucoup plus généraux et visent un ensemble d'éléments (voir par exemple le guide de Schaub et Biery 1998). Plusieurs auteurs proposent dans leur ouvrage des listes de contrôle ou des éléments à vérifier (Momboisse 1968; Kingsbury 1973; Hess et Wrobleski 1992; Floyd 1995; Geiber et Nasset 1998; Berger 1999; Broder 2000; Kovanich 2003; Sennewald 2003; Fisher et Green 2004; Fennely 2004). En les consultant, l'expert ne doit pas chercher à trouver LE guide, mais bien à s'inspirer de ceux-ci afin d'en développer un adapté à l'organisation qu'il souhaite inspecter et au mandat établi au départ (Walsh et Healy

1994 : 2-I-10; Johnson 2005 : 341-342; Gagnon 2006 : 29). Il est risqué d'utiliser un guide qui n'est pas adapté à une organisation. Il ne s'agit pas d'un outil rigide et il peut être modifié tout au long du projet si l'expert juge qu'il y a eu des aspects importants qui n'ont pas été intégrés dès le départ. Tout comme l'organisation, il peut évoluer et se modifier d'un audit à l'autre (Gagnon 2006 : 29). Des éléments obsolètes peuvent devenir plus importants et vice-versa.

Le guide peut être conçu de manière à procéder à l'examen de l'organisation de l'extérieur vers l'intérieur (Geiben et Nasset 1998 : 98; Kovanich 2003 : 187). Ce type d'examen est aussi proposé par Johnson (2005 : 333-334). Ce dernier compare l'audit à un oignon à couches multiples. La première couche comprend l'environnement extérieur et la région dans laquelle l'organisation se situe. Les couches qui suivent peuvent inclure la ville et le quartier où se trouvent les installations. Par la suite, l'examen porte sur le périmètre extérieur, sur les accès et les bâtisses. L'examen se poursuivra jusqu'au cœur de l'organisation. Le National Crime Prevention Institute propose l'inverse et suggère de structurer l'audit en commençant par le cœur des opérations et par les actifs importants qui sont le plus à risque (NCPI 1986 : 47). Pour établir quels sont ces actifs, il suggère de tenir compte de la perte maximale possible et de la perte maximale probable.

Pour Garcia (2001 et 2006), les listes de contrôle sont utilisées pour vérifier la présence ou l'absence de composante de sécurité (équipement, procédure et personnel) servant à protéger les actifs ayant une faible valeur. Pour protéger les actifs vitaux de l'organisation et pour vérifier la réelle efficacité du système de sécurité, Garcia recommande d'évaluer la performance et l'efficience des composantes de sécurité en les testant. Par exemple, il est possible de tester un portique conçu pour détecter le métal en le franchissant à plusieurs reprises avec un objet sensé être détecté. Après ce test, le professionnel obtient des statistiques sur le bon ou le mauvais fonctionnement de la composante (exemple : un objet détecté 19 fois sur 20 ou à 95 %). Cette statistique jumelée à un intervalle de confiance permet d'établir les probabilités qu'une personne qui traverse le portique avec un objet de métal soit détectée (Garcia 2006 : 7).

1.5.3 La cueillette des données

Après avoir réalisé la visite préliminaire et s'être préparé, l'expert est prêt pour la cueillette des données. Elles sont collectées de plusieurs sources (Leman-Langlois et Dupuis 2007 : 442).

Les données provenant des sources extérieures à l'organisation sont recueillies (Kingsbury 1973 : 13-18; Cusson, Tremblay, Biron, Ouimet et Grandmaison 1994 : chapitre 4; Roper 1997 : 31-32; Tucker 2000 : 92-93; Johnson 2005 : 347). Il peut s'agir de données policières qui aident à comprendre le crime dans le secteur (exemples : taux de criminalité, distribution du crime dans le temps et dans l'espace, types de crimes commis et rapports d'incidents). Il peut aussi s'agir de données amassées par des organisations similaires à celle auditée (historique des incidents) ou de statistiques disponibles auprès des compagnies d'assurances.

Il est possible de colliger des données internes relatives aux incidents passés. Nous pensons par exemple à l'historique des incidents passés et aux rapports d'incidents. Les rapports d'inventaire qui permettent d'estimer les pertes encourues par l'entreprise peuvent aussi être consultés. Il y a deux problèmes reliés aux données relatives aux incidents passés (Walsh et Healy 1994 : 2-I-7). Elles ne sont pas toujours disponibles et l'organisation des informations ne permet pas toujours de faire des analyses statistiques. Cette situation est défavorable puisqu'en traitant ces informations il est plus facile pour un expert de prévoir les incidents futurs (Walsh et Healy 1994 : 2-I-7; Leman-Langlois 2007 : 370). Plus il y aura de données à analyser et plus les prédictions risquent d'être précises (Walsh et Healy 1994 : 2-I-8). Puisque les organisations ne compilent pas toujours rigoureusement ces données, l'expert n'a parfois d'autre choix qu'opter pour une approche différente et aller sur les lieux pour constater par lui-même les faits et pour rechercher les informations pertinentes (ASIS International 2003 : 10-11).

L'auditeur s'informe auprès du personnel et des contractants qui travaillent pour l'organisation (Johnson 2005 : 348). Puisqu'il est impossible et inutile de rencontrer tous les employés, il sélectionne les personnes clés en fonction de leurs connaissances et de leur position (Sennewald 1989 : 48). Elles pourront répondre aux questions posées oralement ou par écrit à l'aide d'un formulaire (Johnson 2005 : 348). Les gens ne sont pas seulement rencontrés pour connaître leur opinion face aux problèmes et pour recueillir des pistes de solution, mais aussi pour vérifier s'ils sont ouverts à l'idée d'implanter des mesures de sécurité dans leur environnement de travail. Il faut éviter d'installer des dispositifs qui seront rejetés par les employés (Cusson 1998 : 44). Le bon fonctionnement d'un système de sécurité repose en partie sur le niveau d'acceptation des employés face aux dispositifs qui sont présents dans leur univers de travail et sur le bon usage qu'ils vont en faire (Cusson 1998 : 44).

Le professionnel examine systématiquement l'organisation : les lieux, les employés et les équipements. Il découvre ainsi les forces et les faiblesses en matière de sécurité. Cette séance d'observation permet de corroborer ou d'infirmer certaines informations qui sont données par les employés. Johnson (2005 : 350) propose trois méthodes d'observation. La première consiste à faire une observation complète sans déranger les activités de l'organisation. Il y a aussi l'observation participante. L'expert participe alors aux activités des personnes observées et des questions relatives à leur travail ou aux opérations peuvent être posées. La troisième forme d'observation est secrète et les employés ne sont pas informés de la présence de l'expert. Ce dernier cherchera à exploiter les vulnérabilités de l'organisation sans être détecté (exemples : tester la vigilance des gardes de sécurité, vérifier si les employés appliquent les procédures, effectuer des tests de pénétration). La direction doit être mise au courant des observations secrètes qui sont réalisées dans le cadre du mandat (Roper 1997 : 35). Idéalement, les visites sont faites à différents moments (exemples : jour, soir, nuit, semaine, fin de semaine, sur les périodes de travail, durant les heures de fermeture) (Roper 1997 : 38).

Des documents sont consultés et analysés : les règlements, les politiques et procédures de l'organisation, les rapports d'audits antérieurs, ainsi que tous les documents contenant des informations ayant un impact sur le niveau de sécurité (Broder 2000 : 63). La lecture des plans du site facilite la compréhension des lieux et les déplacements lors de l'observation sur le terrain (Johnson 2005 : 338).

Il teste les dispositifs de sécurité déjà en place. Il peut s'agir de tests rapides ou de tests plus élaborés comme ceux proposés par Garcia (2006). Le premier type de test est fait rapidement et facilement. Par exemple, il peut tester un système d'alarme pour vérifier s'il fonctionne ou s'il est désuet. Étant plus coûteuse en temps et en argent, la réalisation des tests plus élaborés doit être convenue dans le mandat initial avec le client.

1.5.4 L'analyse des données

Après avoir rassemblé toutes les données, le professionnel procède à leur analyse dans le but de connaître le niveau de sécurité de l'organisation, ses problèmes, ses risques et de recommander des solutions appropriées. En sécurité privée, l'analyse apparaît comme le point faible de l'audit de sécurité. L'expert qui sait traiter, analyser et interpréter les données sera davantage en mesure de recommander des actions efficaces pour améliorer la sécurité (Leman-Langlois 2007 : chapitre 25).

Parmi les analyses recommandées par Clarke et Eck (2003 : chapitres 20 à 31) se trouve l'identification des endroits où les incidents se concentrent (Clarke et Eck 2003 : chapitre 21). Il n'est pas rare que les vols, les intrusions, les crimes ou les autres incidents soient nettement plus fréquents à certains endroits qu'ailleurs. Cette analyse permet de constater que l'organisation est située dans un quartier chaud ou s'il y a des endroits précis sur le site où il y a une concentration d'incidents. Quand de tels points chauds sont découverts, la recommandation qui s'impose est de concentrer les efforts à ces endroits (Cusson 2002 : 176-179). Il peut être intéressant de cartographier les incidents à l'aide d'un logiciel conçu à cette fin pour visualiser facilement les points

chauds. Il faut tenter d'utiliser les cartes les plus détaillées possible, surtout sur les sites ayant de petites ou de moyennes superficies (Rengert et coll., 2001 : 97 et ss.). Par exemple, des cartes en trois dimensions permettent de cartographier des incidents sur tous les étages d'un édifice en hauteur. Les incidents peuvent aussi être situés dans le temps. Est-ce qu'il y a des heures, des jours, des saisons ou des années plus problématiques que d'autres ? Dans l'éventualité où l'expert constate des concentrations dans le temps, il s'interroge sur les raisons qui les expliquent et développe des mesures en fonction de ces périodes plus problématiques.

Il est intéressant de découvrir les raisons pour lesquelles certaines organisations sont plus à risque que les autres (Clarke et Eck 2003 : chapitre 26). Par exemple, une organisation peut avoir en sa possession des produits convoités vulnérables au vol. Le professionnel identifie les « points et les produits chauds » et met en place des mesures qui visent à dissuader les personnes malintentionnées de s'attaquer à ces endroits et à ces produits (Clarke et Eck 2003 : chapitre 29). Des méthodes dont l'efficacité a été démontrée peuvent être choisies afin de régler des problèmes spécifiques de sécurité. Plusieurs actions, notamment les mesures utilisées en prévention situationnelle, découragent les gens malhonnêtes de s'attaquer à une organisation et à ses actifs (Clarke et Eck 2003 : Cusson 2007 : chapitres 27, 28, 29 et 31). Par exemples, la présence d'un gardien et d'un système d'alarme augmentent les risques d'être détecté.

Les ouvrages consacrés à la sécurité privée proposent aussi des éléments à prendre en considération lorsque vient le temps d'analyser les données et de prendre des décisions face aux risques identifiés. L'expert tient compte d'un certain nombre de contraintes lorsqu'il effectue ses recommandations et il fait des compromis (Fisher et Green 2004 : 138). Par ailleurs, le fait de recommander des mesures dispendieuses sans tenir compte des contraintes budgétaires de l'entreprise peut inciter les gestionnaires à rejeter les recommandations.

Il est aussi recommandé d'effectuer une analyse coût/bénéfice pour identifier les avantages et les inconvénients rattachés à chacune des mesures de sécurité (Broder

2000 : chapitre 5). Il est déconseillé de recommander des mesures importantes de sécurité pour des problèmes mineurs ou de se protéger au-delà des pertes maximales probables (NCPI 1986 : 47). Il faut aussi tenter de maintenir les coûts reliés à la sécurité aussi bas que possible et, éventuellement, de réaliser un bénéfice égal ou supérieur au coût du dispositif (NCPI 1986 : 51).

Après avoir identifié les risques, le professionnel établit des priorités et choisit les mesures appropriées (Broder 2000). Pour établir ses priorités, il peut tenir compte des probabilités et du niveau de gravité de chacun des risques (Johnson 2005 : 353). Par la suite, il détermine aussi l'ordre dans lequel les mesures seront mises en place. Qu'est-ce qui doit être fait immédiatement ? Qu'est-ce qui peut attendre ?

Même si des mesures ont pour but d'éliminer ou de réduire certains risques, il y a toujours un risque résiduel. Il s'agit de la portion du risque qui demeure même si des mesures de sécurité sont prises. Le risque résiduel va être plus ou moins important selon les actifs qui doivent être protégés ou les personnes qui ont à les maîtriser.

1.5.5 La rédaction du rapport

La dernière étape consiste en la rédaction et la présentation du rapport. En nous basant sur le style de rapport établi par Broder (2000 : 70-71), nous proposons un plan divisé en sept parties : le sommaire exécutif, l'introduction, la connaissance du milieu, le mandat, la démarche adoptée pour réaliser l'audit, les constats et les recommandations, et, finalement, la conclusion.

Il est préférable d'inclure un sommaire exécutif au rapport. Les hauts gestionnaires ont souvent peu de temps à accorder à la lecture du rapport et le sommaire est un outil qu'ils apprécient.

En guise d'introduction, le projet et le rapport sont présentés.

Une partie intitulée « la connaissance du milieu » peut être introduite. Le but n'est pas de faire connaître l'organisation au demandeur puisqu'il la connaît déjà. Ce qui est recherché, c'est de lui démontrer que l'expert la connaît bien. Cette partie est utile pour les consultants externes qui réalisent un mandat pour un client ou pour un gestionnaire en sécurité récemment embauché dans une organisation.

Le mandat est précisé afin que les lecteurs comprennent le travail qui a été réalisé. Il est préférable d'expliquer ce qui a été inclus et exclu du mandat.

Dans la cinquième partie, l'expert décrit la démarche adoptée. Il mentionne la durée du projet, décrit sa méthodologie et sa cueillette des données.

Sixièmement, il décrit les constats et recommande des mesures pour faire face aux problèmes. Quelles sont les menaces pesant sur l'organisation ? Quels sont les actifs non protégés ? Quelles sont les vulnérabilités observées ? Y a-t-il des protections déjà en place qui doivent être modifiées, améliorées ou supprimées ? Quel est le niveau de sécurité de l'entreprise ? Quels sont les risques en matière de sécurité ? Il est suggéré d'introduire des photos pour appuyer les constatations. Il n'est pas nécessaire d'attendre à cette étape pour informer l'organisation d'un problème grave. Les responsables doivent être avisés dès qu'un tel problème est constaté pour que des mesures soient prises le plus tôt possible (Gagnon 2006 : 98). Il faut toutefois faire mention de ces problématiques dans le rapport final et expliquer les mesures qui ont été suggérées et retenues (Roper 1997 : 34).

Suite aux constats, l'expert fait ses recommandations. Selon les probabilités et l'impact, il suggère des décisions à prendre pour chacun des risques. Est-il préférable d'accepter, de transférer, de distribuer, de diminuer ou d'éliminer le risque ? Faute de moyens, il n'est pas possible ni recommandé pour une organisation de viser à éliminer et réduire tous les risques. L'expert suggère d'éliminer et de réduire les risques susceptibles d'affecter les actifs importants et stratégiques de l'organisation. Il

recommande les contre-mesures appropriées. Quatre catégories de contre-mesures sont proposées par Sennewald (2003 : 185-186).

La première catégorie englobe tout ce qui se rapporte au matériel de sécurité (exemples : porte, serrure, coffre, barrière, mur). Les systèmes électroniques constituent la deuxième catégorie (exemples : caméra, biométrie, système d'alarme). La troisième catégorie est l'implantation de procédures de sécurité ou la modification de ces dernières (exemples : recommander qu'un inventaire soit réalisé sur une base plus régulière ou tenir des inventaires plus petits pour les produits de valeur). La quatrième catégorie concerne le personnel affecté à la sécurité. Cette solution est envisagée en dernier recours parce qu'elle est la plus coûteuse (Sennewald 2003 : 183-186). De plus, l'efficacité de cette dernière dépend grandement de la compétence et de l'intégrité des personnes engagées. La meilleure protection consiste donc en une combinaison et une interaction de différentes mesures adaptées à l'organisation (NCPI 1986 : 56; Cusson 1998 : 44).

Il ne faut toutefois pas se restreindre à ces quatre catégories de contre-mesures. Il faut laisser place à l'imagination de l'expert. Certaines actions qui ne sont pas incluses dans ces catégories peuvent très bien régler un problème de sécurité. Par exemple, une campagne de sensibilisation auprès des employés peut avoir comme effet de faire diminuer le nombre de crimes dans une entreprise. En usant de son imagination, il peut trouver des solutions innovatrices et intéressantes pour régler les problèmes auxquels il fait face (Leman-Langlois 2007 : 382-385).

Il faut aussi tenir compte des effets négatifs que certaines actions peuvent avoir sur une organisation et tenter de causer le moins de désagréments possible aux opérations de l'organisation (Cusson 1998 : 34 et 44; Leman-Langlois 2007 : 383-384). La sécurité parfaite est un concept hypothétique et se rapprocher de la perfection est théoriquement réalisable, mais très difficilement praticable (Berger 1999 : 22). L'expert doit être en mesure de trouver des mesures qui rendront l'environnement sécuritaire sans trop nuire aux opérations, à la liberté et au moral des travailleurs

(Cusson 1998 : 44; Berger 1999 : 22). Certaines interventions normalement efficaces peuvent s'avérer inefficaces si elles ne sont pas compatibles avec le type d'organisation, ses opérations ou si elles ne sont pas acceptées par les employés de l'entreprise.

En guise de conclusion, les éléments importants du projet sont soulevés.

La rédaction du rapport est une étape importante puisque ce dernier est lu et éventuellement critiqué par les demandeurs du projet. Ce document doit être de bonne qualité, doit être facile à lire, logique, clair et consistant (Broder 2000 : chapitre 8; Johnson 2005 : 352). Les paragraphes longs et compliqués sont à proscrire. Les termes techniques doivent être définis pour que tous puissent être en mesure de comprendre le contenu (Johnson 2005 : 353). Bien que certains experts puissent redouter la rédaction du rapport (Broder 2000), il faut y mettre les efforts nécessaires afin de livrer un produit représentatif du travail effectué sur le terrain. Idéalement, le document est présenté et discuté lors d'une rencontre entre l'expert et les différents intéressés (Kingsbury 1973 : 228; NCPI 1986 : 52).

1.6 L'après audit

À l'aide du rapport, le demandeur est maintenant en mesure de décider des actions qui s'imposent pour atteindre le niveau de sécurité désiré (Gagnon 2006 : 127-128). C'est lui seul qui décidera de suivre ou non les recommandations. L'expert demeure disponible pour répondre à ses questions et, si nous lui demandons, vérifier ce que l'audit a permis de réaliser. Le demandeur peut souhaiter être accompagné dans l'implantation des contre-mesures. Il peut s'agir de « magasiner » les fournisseurs de biens et services pour lui, de vérifier les prix ou de l'aider à rédiger des procédures de sécurité.

Plusieurs recommandations peuvent être retenues et il est souvent impossible de prendre action immédiatement pour chacune d'elles. Cela est principalement dû au

facteur temps et au manque d'argent. Les actions peuvent s'échelonner sur quelques mois, voire quelques années. Construire un plan d'action va aider à structurer l'implantation des mesures de sécurité retenues, de déterminer les priorités et à établir un échéancier (Gagnon 2006 : 130-132).

Éventuellement, une visite est prévue pour vérifier quelles sont les recommandations qui ont été retenues et implantées suite à l'audit (Kingsbury 1973 : 228). Est-ce que les mesures donnent de bons résultats ? Qu'est-ce qui ne fonctionne pas ? Est-ce qu'il y a des modifications ou des ajouts à apporter ? Dans l'éventualité où l'organisation est victimisée suite au projet, il est conseillé de se rendre sur les lieux et de vérifier comment l'évènement s'est produit et de constater les pertes subies (NCPI 1986 : 52).

Ultérieurement, une évaluation est réalisée dans le but de vérifier si les dispositifs mis en place sont réellement efficaces et s'il y a des résultats concrets. Cette évaluation peut être basée sur la perception des gens sur le terrain, mais il est préférable de l'appuyer sur des chiffres. C'est ici que la quantification des pertes et des évènements va permettre une mesure plus exacte et une évaluation plus précise de l'impact des solutions mises en place (Cusson 1998 : 44). L'expert tient compte de quatre éléments pour effectuer cette évaluation (Cusson et coll. 1994 : 40-41). Premièrement, il faut définir les deux périodes d'analyse. Dans notre cas, il s'agit de comparer la période qui précède et celle qui suit l'implantation des mesures de sécurité. Deuxièmement, il faut définir les éléments qui serviront de critères afin d'évaluer l'effet des mesures mises en place (exemples : total des pertes subies avant et après, nombre d'incidents avant et après). Troisièmement, il faut être capable de décrire de façon précise l'intervention qui a été posée par l'expert et l'organisation suite à la réalisation de l'audit. Quelles sont les mesures exactes qui ont été mises en place ? À partir de quel moment ont-elles été opérationnelles ? Finalement, des données comparatives peuvent être utilisées pour vérifier si l'impact mesuré est réellement dû aux interventions effectuées ou s'il est le résultat de facteurs exogènes sur lesquels l'organisation n'a pas de contrôle.

Ce suivi pour évaluer l'efficacité du projet et des correctifs se doit d'être fait par une personne compétente, mais surtout honnête. Idéalement, ce suivi devrait être fait par une personne indépendante (Leman-Langlois et Dupuis 2007 : 447). Il est important d'éviter les évaluations complaisantes qui pourraient être faites par l'expert qui a réalisé l'audit ou encore par les personnes responsables des mesures mises en place. « Mieux vaut un constat d'inefficacité après une procédure rigoureuse qu'une impression d'efficacité jamais réellement démontrée » (Leman-Langlois et Dupuis 2007 : 448). Il est préférable que l'expert accepte un échec qu'il s'entête à dire que le projet est une réussite si ce n'est pas le cas. Un des objectifs de l'évaluation est justement de corriger le tir en cas de problème.

Au cours de l'évaluation, il peut s'avérer intéressant de vérifier s'il n'y aurait pas eu un déplacement du problème dans l'organisation. Le phénomène de déplacement peut être observé de cinq façons (Felson et Clarke 1998 : 25). Premièrement, le problème peut se déplacer d'un endroit à un autre (déplacement géographique). Deuxièmement, le déplacement peut s'opérer dans le temps (déplacement temporel). Troisièmement, en s'apercevant qu'une cible est efficacement protégée, les infracteurs peuvent décider de s'attaquer à d'autres cibles qui ne sont pas aussi bien protégées (Cusson 2000 : 132). Quatrièmement, ils peuvent décider d'utiliser d'autres moyens pour s'attaquer aux mêmes cibles (Cusson 2000: 132). Finalement, les criminels peuvent délaisser un crime pour un autre. Quoique l'analyse du déplacement soit intéressante et qu'il soit profitable de se pencher sur cette question, ce phénomène a souvent été exagéré (Killias 1991 : 331; Felson et Clarke 1998 : 25-29). Il est faux de croire que les crimes que nous réussissons à prévenir en protégeant un site ou une cible vont tous se déplacer d'une forme ou d'une autre. L'inverse peut aussi être observé puisqu'il y a à l'occasion une diffusion des bénéfices (Felson et Clarke 1998 : 30-32). Des actifs non visés par les mesures et non protégés peuvent bénéficier de la protection des dispositifs installés pour les actifs environnants.

L'audit est, en principe, un exercice qui est répété périodiquement (Mombroisse 1968 : 30-31; Broder 2000 : 3; Johnson 2005 : 334). Étant dynamiques, les entreprises

changent et les risques évoluent. Un actif qui autrefois n'était pas attrayant peut le devenir (exemple : la hausse du prix de l'or peut faire en sorte que des mineurs soient davantage incités à voler leur employeur). Avec le temps, le niveau de sécurité d'une organisation change. Des mesures inexistantes ou hors de prix à un moment donné apparaissent ou sont offertes plus tard à un prix abordable. Par exemple, l'évolution de la technologie fait apparaître de nouveaux systèmes et fait baisser les prix.

2. PROBLÉMATIQUE

En parcourant la littérature spécialisée (principalement anglophone), nous nous sommes aperçus que plusieurs experts ont écrit au sujet du « security survey ». La plupart de ces auteurs sont des membres de l'association ASIS International et proposent des façons similaires de réaliser l'audit de sécurité. Dans la recension des écrits, nous avons aussi présenté des ouvrages rédigés par des criminologues s'étant intéressés aux concepts du contrôle social, de la prévention situationnelle et de la dissuasion. L'audit de sécurité a été présenté dans une perspective d'analyse et de gestion des risques. Tous ces ouvrages et ces concepts sont susceptibles d'intéresser les experts qui ont à faire des audits de sécurité dans le cadre de leur travail. Si la littérature spécialisée permet de peaufiner la méthode utilisée pour réaliser le projet, les concepts théoriques quant à eux aident à mieux comprendre et analyser les problèmes de sécurité.

Un mémoire portant sur l'audit de sécurité va nous permettre d'approfondir les connaissances dans ce champ d'études et de dresser un portrait sur ce qui est accompli en cette matière par les personnes chargées de la sécurité des organisations dans la grande région de Montréal. Nous nous intéresserons principalement aux méthodes qu'elles utilisent pour le réaliser et vérifierons si elles utilisent les ouvrages exposés dans la recension des écrits.

Question de recherche

Est-ce que les experts utilisent la littérature spécialisée ainsi que les concepts retrouvés dans les théories du contrôle social, de la prévention situationnelle et de la dissuasion lorsqu'ils effectuent un audit de sécurité ?

3. MÉTHODOLOGIE

Dans ce chapitre, nous expliquons la méthodologie qui a été utilisée pour réaliser cette recherche. L'objet et les objectifs de la recherche sont exposés. Par la suite, nous donnons de plus amples informations sur la démarche que nous avons utilisée pour recueillir les données, sur les données elles-mêmes et finalement sur l'analyse que nous avons effectuée de ces dernières.

3.1 Objectifs de la recherche

Pour ce qui est des fins de cette recherche, nous avons un objectif général et quatre objectifs spécifiques qui sont les suivants :

Objectif général

-Analyser les audits de sécurité effectués par les acteurs chargés de la sécurité et vérifier s'ils utilisent la littérature spécialisée ainsi que les théories développées en criminologie.

Objectifs spécifiques

-Identifier les méthodes qui peuvent être utilisées pour réaliser les audits de sécurité.

-Analyser et comprendre les étapes qui peuvent être suivies par les acteurs lorsqu'ils procèdent à un audit de sécurité pour une organisation.

-Analyser la terminologie en lien avec l'audit de sécurité utilisée par les acteurs dans le but de choisir et de proposer nos propres termes.

-Comprendre le contexte lié à l'audit de sécurité.

3.2 Délimitation de l'objet d'étude

Dans le cadre de cette recherche, nous nous sommes limités à rencontrer des personnes qui travaillent pour des entreprises privées. Certaines d'entre elles avaient déjà travaillé pour des organisations publiques dans le passé. D'autres exécutent des mandats pour des clients qui sont des entités publiques ou parapubliques. Plusieurs s'inspirent de concepts développés par des employés du gouvernement (exemples : Gendarmerie Royale du Canada et Homeland Security aux États-unis). Au moment où nous avons rencontré ces gens, ils travaillaient tous pour une entreprise privée.

Certains professionnels ne font pas une analyse rigoureuse quand ils font un relevé de sécurité. Les besoins des clients sont parfois pris pour acquis et les recommandations sont faites avec un minimum d'analyse. Nous sommes conscients que ce ne sont pas tous les experts qui utilisent une méthode et qui font une analyse rigoureuse lorsqu'ils auditent une organisation. Par exemple, un vendeur de caméras de surveillance peut recommander l'installation d'un système de télésurveillance sans s'interroger sur l'efficacité réelle de ce système. Broder (2000) donne l'exemple d'une entreprise qui a installé des caméras extérieures dans un secteur où il y a du brouillard 6 mois par année. L'efficacité de ce système dans un environnement semblable est discutable. Pour notre mémoire, nous avons cherché à rencontrer des gens qui ont une méthode de travail et qui font un minimum d'analyse.

Dans ce domaine, nous retrouvons des audits généraux qui touchent à l'ensemble de la sécurité. D'autres sont beaucoup plus spécifiques et se limitent à vérifier des éléments plus précis dans l'organisation (exemples : informatique, comptabilité, réception et expédition). Nous limitons notre recherche aux audits généraux.

3.3 Sélection du corpus empirique

3.3.1 Constitution du corpus

Pour constituer notre échantillon, nous avons consulté les bottins conçus par des étudiants de l'École de criminologie. Beaucoup d'experts y sont répertoriés et nous avons trouvé les coordonnées pour les contacter. Il y a une description des principales tâches qui sont accomplies par ces gens. Dans l'un des bottins, il y a aussi le niveau d'intérêt des milieux à accueillir un stagiaire. Nous avons présumé qu'un milieu ouvert à l'arrivée d'un stagiaire provenant de l'École de criminologie était plus enclin à fournir une entrevue dans le cadre d'une recherche. Des gens susceptibles de faire des relevés de sécurité ont par la suite été contactés. Avant de communiquer avec les personnes, nous regardions s'il y avait des informations supplémentaires disponibles sur Internet concernant leur entreprise. En premier, un courriel a été envoyé aux candidats sélectionnés pour évaluer l'ouverture qu'ils avaient vis-à-vis notre projet. Les gens ayant répondu positivement ont par la suite été contactés par téléphone. Il s'agissait alors d'évaluer s'ils étaient en mesure de nous aider et de planifier une rencontre.

Nous avons aussi participé aux activités organisées par l'organisation ASIS International (chapitre Montréal). Le chapitre de Montréal regroupe plusieurs responsables de la sécurité, dont plusieurs gestionnaires. Les membres de Montréal organisent régulièrement des activités (exemples : conférences, formations, forums virtuels). En participant à ces activités, nous avons eu la chance de côtoyer des responsables de sécurité oeuvrant dans des entreprises privées de la grande région de Montréal. Nous avons interviewé quelques personnes parmi les membres du chapitre de Montréal.

Finalement, une partie de l'échantillon a été bâtie à l'aide de la technique « boule de neige » (Pires, 1997). Il nous a été possible de rencontrer trois experts à l'aide d'informations fournies par d'autres professionnels que nous avions rencontrés au

préalable. Certaines personnes sont difficiles à joindre et nos contacts nous ont donné leurs noms ainsi que leurs coordonnées.

Tout au long du projet, différents experts ont contribué à enrichir nos données. Pour faciliter la lecture du mémoire et sa compréhension, nous tenons à présenter les experts et leur contribution respective dans le présent mémoire :

1. Gérald : Expert qui travaille à l'interne pour une entreprise privée. Il est l'un des conférenciers de la soirée ASIS portant sur notre sujet d'étude. Nous avons enregistré et transcrit un verbatim de sa conférence.
2. Dimitri : Expert qui travaille pour une entreprise qui offre des services-conseils en sécurité. Il est l'un des conférenciers de la soirée ASIS portant sur notre sujet d'étude. Nous avons enregistré et transcrit un verbatim de sa conférence.
3. Pierre : Expert qui travaille pour une entreprise qui offre des services-conseils en sécurité. Il est l'un des conférenciers de la soirée ASIS portant sur notre sujet d'étude. Nous avons enregistré et transcrit un verbatim de sa conférence.
4. James : James travaille pour un service interne de sécurité pour une entreprise et offre aussi des services-conseils pour d'autres organisations à l'occasion. Il a donné une conférence lors de la soirée ASIS que nous avons par la suite analysée. Il a été rencontré lors d'un entretien. Nous l'avons aussi accompagné sur un site lors d'un audit (observation) et finalement il nous a partagé le rapport qui a découlé de cette visite.
5. Myriam : Elle travaille pour un service interne de sécurité d'une organisation et offre aussi à l'occasion des services-conseils. Myriam est la collègue de James et elle était présente lors de la séance d'observation.
6. Cynthia : Elle travaille pour une entreprise qui offre des services-conseils en sécurité. Elle nous a offert un entretien. Nous l'avons accompagné sur le terrain (observation). Elle a partagé deux rapports que nous avons analysés.
7. Peter : Stagiaire en criminologie qui nous a partagé un rapport de stage (audit de sécurité qui a réalisé lors d'un stage).
8. Simon : Stagiaire en criminologie qui nous a partagé un rapport de stage (audit de sécurité qui a réalisé lors d'un stage). Il travaille maintenant pour une entreprise qui offre des services-conseils en sécurité. Il a aussi été rencontré lors d'un entretien et nous avons analysé un cas ensemble.
9. Édouard : Il travaille pour une entreprise qui offre des services-conseils en sécurité. Il nous a offert un entretien.
10. Valérie : Elle travaille dans un service de sécurité interne d'une entreprise. Elle nous a offert un entretien.
11. Carol : Il travaille à son compte et offre des services-conseils en sécurité. Il nous a accordé un entretien.
12. Sylvio : Il travaille pour un service de sécurité interne d'une entreprise. Il nous a accordé un entretien.

13. Karine : Elle travaille pour un service de sécurité interne d'une entreprise. Elle nous a accordé un entretien.
14. Sébastien : Il travaille pour un service de sécurité d'une entreprise. Il nous a accordé un entretien.
15. Ralph : Il travaille pour un service de sécurité d'une entreprise. Il nous a accordé un entretien.
16. Kevin : Expert qui travaille pour une entreprise qui offre des logiciels informatiques spécialisés en sécurité privée. Il nous a accordé un entretien téléphonique. Des questions lui ont été posées sur l'apport que ces logiciels pouvaient apporter à l'audit de sécurité.

Au total, seize experts ont été impliqués dans notre cueillette des données. Cet ensemble de données constitue notre corpus empirique.

3.3.2 Saturation empirique des données

Nous avons arrêté la collecte des données au moment où nous avons jugé que le niveau de saturation empirique recherché était atteint (Pires, 1997). Lorsque nous avons jugé que les entretiens, l'analyse des cas et les observations ne nous amenaient plus suffisamment d'informations nouvelles sur notre sujet, nous avons arrêté de recueillir des données. Après l'implication de 15 experts dans notre projet, nous croyions à ce moment avoir assez de matériel pour réaliser notre analyse. Un seul entretien a suivi et il s'agit de l'entretien téléphonique que nous avons eu avec Kevin. Il nous manquait alors des informations au sujet des logiciels spécialisés en sécurité utilisés lors des audits.

3.3.3 Diversification des données

La diversification externe de l'échantillon s'est faite en rencontrant des gens qui travaillent pour des agences de sécurité contractuelles ou pour des services internes de sécurité des entreprises privées. Nous avons diversifié ces deux groupes à l'interne. Le premier groupe (agences de sécurité contractuelles) a été diversifié à l'aide d'un facteur. Nous avons rencontré des gens qui travaillent pour des agences qui offrent exclusivement de la consultation en matière de sécurité et d'autres qui travaillent pour des entreprises qui offrent à la fois des services-conseils et d'autres services et biens

reliés à la sécurité. Nous pensons que le fait d'offrir des services et des biens peut avoir un impact sur la façon de faire un audit de sécurité. En effet, il est possible que le travail soit dirigé en fonction de la vente éventuelle d'un bien ou d'un service.

Le deuxième groupe (services internes des entreprises) a été diversifié en tenant compte de la position occupée par l'interviewé (employé ou gestionnaire). Le poste occupé par la personne peut jouer sur sa façon de travailler, d'analyser la sécurité et sur les recommandations proposées.

Nous avons rencontré des membres d'ASIS International et des personnes qui n'étaient pas affiliées à cette organisation. Nous croyons qu'être membre de l'ASIS International peut amener les professionnels à réaliser les audits de sécurité d'une façon similaire.

3.4 Méthodes de cueillette des données

La principale méthode de cueillette des données est l'entretien semi-directif de type qualitatif. De plus, nous avons eu la possibilité d'utiliser deux autres méthodes accessoires pour compléter les entretiens. Il s'agit de l'observation participante et de l'analyse de cas réels. Cinq experts nous ont offert de les accompagner dans leur travail ou d'analyser des dossiers d'audits qu'ils avaient effectués dans le passé. Nous avons pu aller rechercher des informations qui n'avaient pas été amassées durant les entretiens. Ces deux techniques de cueillette des données nous ont aussi permis de vérifier s'il y avait un décalage entre le discours des interviewés et leur pratique sur le terrain (Diaz, 2005). Le choix de l'observation et de l'analyse de cas se justifie aussi par le fait que notre objet d'étude comporte des aspects très techniques qui ont été plus faciles à percevoir en les observant. La recherche qualitative nous a permis de combiner ces trois méthodes pour collecter nos données (Deslauriers et Kérisit, 1997). La méthodologie qualitative permet d'appréhender et de comprendre le travail des professionnels de la sécurité privée lorsqu'ils effectuent des audits de sécurité en leur accordant une place centrale dans la recherche (Michelat, 1975).

3.4.1 Les entretiens semi-directifs

L'entretien semi-directif est une technique qui permet d'accorder une place importante aux professionnels (Michelat, 1975 ; Poupart, 1997). En leur donnant la plus grande liberté possible durant les entretiens, ils peuvent aborder les éléments qu'ils jugent importants. Ce genre d'entretien permet de traiter notre sujet d'étude en profondeur en allant chercher des informations détaillées et une meilleure connaissance du travail effectué par les experts (Michelat, 1975). Au total, 11 experts nous ont accordé un entretien.

Thèmes investigués durant les entretiens

Voici les principaux thèmes qui ont été abordés durant les entretiens :

-Terminologie utilisée par l'expert pour décrire le projet à l'étude
-Contexte qui explique la demande d'audits de sécurité
-Méthodologie utilisée pour réaliser le travail (étapes à suivre)
-Collecte d'informations et de données durant l'audit
-Éléments à inspecter durant le projet
-Utilisation d'outils, d'ouvrages et de recherches
-Analyse des données qui est effectuée
-Utilité de faire des audits de sécurité

Consigne de départ

Après quelques entretiens et après nous être aperçu que les experts n'utilisaient pas le terme 'inspection de sécurité', nous avons décidé de discuter de la terminologie au début des entretiens qui ont suivis. Cette introduction dans les entretiens qui ont suivis avait pour but de trouver le terme utilisé par nos interviewés pour décrire le projet que nous nommions au départ 'inspection de sécurité'. Nous procédions à cette introduction en posant des questions ouvertes au sujet des différents termes qui

pouvaient être utilisés. La question était structurée ainsi : « Est-ce que vous utilisez le terme inspection de sécurité, si oui, pouvez-vous me dire qu'est-ce que vous entendez par inspection de sécurité ? » La même question était posée pour définir les termes suivants : audit de sécurité, visite de sécurité, étude de sécurité et évaluation de sécurité. À partir du moment où nous nous entendions sur le terme à utiliser, nous poursuivions l'entretien avec la consigne de départ suivante :

« Comment procédez-vous lorsque vous effectuez une inspection de sécurité ? » ('Inspection de sécurité' pouvait être remplacé par le terme utilisé par l'interviewé)

Cette question ouverte laissait beaucoup de liberté aux interviewés quant aux thèmes qu'ils souhaitaient aborder vis-à-vis notre sujet de recherche. Nous sommes conscients que la discussion sur la terminologie au départ pouvait avoir un effet structurant sur le discours des interviewés. Toutefois, nous avons jugé préférable d'avoir cette discussion pour éviter l'ambiguïté vis-à-vis des termes que nous utilisions. Il était important pour nous de nous adapter aux termes couramment utilisés par le sujet et de connaître son opinion sur cette terminologie.

3.4.2 L'analyse de cas

L'analyse de cas a été basée essentiellement sur la lecture de quatre rapports d'audits ayant été complétés par trois experts. Nous avons eu la chance de lire ces rapports et d'interroger les experts. Deux d'entre eux nous ont permis de consulter les rapports en leur présence. Ils étaient ouverts à répondre à nos questions et beaucoup de notes ont été prises. L'un d'eux nous a autorisé à enregistrer la conversation. Un verbatim de cet entretien a été transcrit et analysé. Le troisième expert nous a procuré une copie intégrale du rapport. Nous avons eu l'opportunité de mieux l'analyser.

Deux étudiants de l'École de criminologie qui avaient réalisé des relevés de sécurité dans le cadre d'un stage nous ont fourni des documents expliquant comment ils ont

procédé pour réaliser leur projet. Ces documents ont été analysés et intégrés à nos données.

3.4.3 L'observation participante

Pour compléter notre cueillette de données, nous avons effectué deux séances d'observation participante. Nous avons accompagné trois experts chargés de faire un audit de sécurité. Cette forme de cueillette de données a consisté à les suivre alors qu'ils faisaient de l'observation sur le terrain. (Peretz 2004 :79) Nous observions le travail qu'ils effectuaient et les clichés qu'ils prenaient. Nous écoutions les échanges qu'ils avaient avec les travailleurs. Finalement, nous participions à la prise de notes. La première séance d'observation s'est déroulée dans une école publique alors que la deuxième s'est déroulée dans un entrepôt de produits finis.

Nous avons aussi participé à une rencontre avec l'un des demandeurs. Les experts lui ont posé les questions qu'ils avaient intégrées à leur guide de sécurité. Cette rencontre fut très intéressante. Le demandeur nous a accompagné pour effectuer la première visite de son entreprise.

Il était permis de noter nos observations et c'est ce que nous avons fait. Nous avons aussi mémorisé le travail qui a été fait par les experts (Peretz 2004 : 81). Une prise de notes a suivi chaque séance d'observation. Nous retranscrivions le maximum d'informations que nous avions captées.

3.4.4 Conférence donnée par ASIS International (chapitre de Montréal)

À l'hiver 2007, une soirée-conférence portant sur notre sujet de recherche a été donnée par le chapitre de Montréal de l'ASIS International. Environ une cinquantaine de membres ont assisté à cette soirée. Il y a eu au total 4 conférenciers invités. Nous avons enregistré la soirée à l'aide d'un enregistreur vocal. Nous avons retranscrit les trois présentations sous forme de verbatim.

Cette soirée fut intéressante et bénéfique à plusieurs niveaux. Premièrement, elle nous a permis de recueillir beaucoup d'informations concernant l'analyse de risques, l'étude de sécurité et l'analyse d'impact d'affaires. Deuxièmement, nous avons rencontré des experts et échangé avec eux sur l'audit de sécurité. Quelques personnes se sont montrées intéressées par notre recherche et nous ont fourni leurs coordonnées pour les joindre. Troisièmement, beaucoup de gens se sont déplacés et semblaient intéressés par les conférences. Cela démontre l'intérêt que les experts portent à ces sujets. Finalement, nous avons pris connaissance du genre d'information que l'ASIS International pouvait transmettre à ses membres et même aux non-membres intéressés par les questions de sécurité. Il est possible que cette soirée puisse avoir eu un impact sur le discours des gens lorsque nous les avons rencontrés par la suite.

3.5 Méthodes d'analyse des données

Pour effectuer l'analyse, nous nous sommes inspirés des textes écrits par Paillé (1994 et 1996) et de Tesch (1990). À l'intérieur de ces textes, nous retrouvons quelques principes généraux forts instructifs qui nous ont aidés à faire l'analyse de nos données qualitatives. Tout comme Tesch, nous ne voyons pas l'analyse comme étant la dernière étape de la recherche. Nous avons commencé l'analyse dès le début de la cueillette des données. Pour débuter, nous rédigions des mémos suite aux entretiens, aux analyses de cas et aux séances d'observation participantes. Chaque mémo contenait une partie plus analytique et une partie descriptive. Ces mémos nous ont permis d'avoir une meilleure connaissance du matériel amassé tout au long de la cueillette de données. Cette réflexion, que nous avons faite dès le début, nous a permis de nous ajuster tout au long de la cueillette des données. Les mémos ont facilité l'analyse horizontale, verticale et transversale.

Tous les entretiens ont été retranscrits intégralement. Dans la mesure du possible, nous avons retranscrit les entretiens au fur et à mesure qu'ils ont été effectués. Cette technique nous a permis de nous imprégner de notre sujet et d'avoir une meilleure

connaissance de notre corpus empirique. L'analyse horizontale et verticale de chaque entretien a donc pu commencer rapidement.

Nous nous sommes inspirés de la démarche proposée par Paillé (1994) pour étudier les verbatim, les mémos et les notes prises au moment où nous avons fait les analyses de cas et les observations. Nous voulions avoir la meilleure connaissance possible et une bonne compréhension de notre sujet d'étude. La démarche d'analyse par théorisation ancrée développée par Paillé permet de réaliser ces objectifs. Les trois premières étapes qui sont la codification, la catégorisation et la mise en relation permettent de mettre de l'ordre dans les données et cela facilite l'analyse. Toutes les données mises ensemble fournissent une somme importante d'informations. En les codifiant et en les catégorisant, il a été plus facile d'en faire l'analyse. Lorsque nous avons terminé d'organiser les données, nous avons obtenu un document d'analyse de 107 pages. Nous avons assemblé tous les passages les plus importants retrouvés dans les verbatims et nous les avons séparés par thèmes, catégories et sous-catégories. Voici la table des matières de ce document :

Terminologie **2**
-Inspection de sécurité 2
-Étude de sécurité 2
-Évaluation de sécurité 3
-Évaluation des besoins 3
-Visite de sécurité 4
-Audit 4
-Risque 6
-Analyse de risque 6
-Confusion 6
-Sécurité vs. Sûreté 8
-Ensemble du projet 8
Échéancier **13**
-Audit : exercice continu 14
Méthodes **16**
Contexte des audits **18**
-Demandeur et pourquoi 18
-Proactivité et réactivité 20
-Problématique 21
-Prise de conscience 22
-Audit de sécurité : la base 22
-Installation et investissement 24
-Manque d'analyse et d'objectivité 27

-Cas Entrepôt Ralphy *27*
-Experts 30
-Service de sécurité interne 32
Préparer l'audit 34
-Connaissance de l'organisation 35
-Entrevue préliminaire 37
-Présentation du projet 39
-Mandat 40
-Limites du mandat 42
-Priorités 44
-Partenaires d'affaires 47
-Guide de sécurité 49
-Guide général et guide spécifique 55
Terrain 56
-Rigueur 56
-Contraintes 56
-Cueillette d'informations 57
-Cueillette des données 60
-Subjectivité dans la recherche des données 66
-Données statistiques 67
-Utilisation de logiciels 71
-Test des systèmes 73
-Prise de photos 74
-Outils utilisés 75
Analyse des experts 75
-Analyse des risques 76
-Analyse des probabilités et impact 78
-Analyse d'impact d'affaires 81
Solutions 81
-Pouvoir décisionnel 87
-Recommandations 89
Rapport 92
-Surprise des gestionnaires 102
-Types de rapport (externe vs interne) 102
Évaluation des résultats 102
-Évaluation du fonctionnement 106

En séparant les verbatims de cette façon, il a été plus facile d'analyser les données et de trouver des pistes d'analyses intéressantes. La mise en relation a finalement permis de faire des liens entre les données. Bien que nous ayons analysé les entretiens à l'aide de thèmes et de catégories, nous les avons aussi étudiés séparément. Nous avons jugé important de faire cette analyse pour situer les données dans leur contexte.

4. LA RÉALISATION D'UN AUDIT DE SÉCURITÉ

Dans ce chapitre, nous commençons par expliquer pourquoi il y a une ressemblance entre les façons de faire les audits décrites dans la recension des écrits et les façons de faire utilisées par les experts que nous avons rencontrés. Par la suite, il est question de la terminologie utilisée pour nommer le projet sous étude et de la confusion qu'il y a ce niveau. Troisièmement, l'audit est situé dans son contexte. Finalement, nous décrivons comment les experts procèdent pour effectuer des audits de sécurité. Pour ce faire, nous utilisons les données que nous avons recueillies soit les entretiens, les analyses de cas et les séances d'observation.

4.1 American Society for Industrial Security (ASIS International)

Dès les premiers entretiens, nous avons été surpris de constater qu'il y avait beaucoup de ressemblances entre les façons de réaliser les audits de sécurité utilisées par les interviewés et les méthodes proposées dans la littérature spécialisée. Les membres d'ASIS International du chapitre de Montréal utilisent les ressources mises à leur disposition par l'organisation. Même s'ils n'étaient pas membres de l'organisation, Peter et Carole utilisaient aussi cette littérature spécialisée pour réaliser leurs projets d'audits. Nous commençons ce chapitre en expliquant pourquoi il y a ces ressemblances.

L'American Society for Industrial Security est une organisation importante pour les professionnels de la sécurité et regroupe présentement plus de 35 000 membres à travers le monde. En date du 10 septembre 2007, cette société comptait 1552 membres au Canada, dont 164 au Québec.

L'une des principales missions de l'ASIS est d'améliorer l'efficacité et la productivité de la pratique de la sécurité (http://www.asisonline.org ainsi que le site http://www.asismontreal.org). Pour ce faire, elle a développé et mis plusieurs outils à la disposition de ses membres. Certains sont aussi disponibles pour les non-membres.

Parmi les outils développés par l'ASIS, nous retrouvons la littérature et les publications, les certifications, les formations et les différentes activités organisées (exemples : séminaires, conférences, forums virtuels).

4.1.1 Certifications offertes par ASIS International

La certification 'Certified Protection Professional' (CPP) est une haute certification en gestion de la sécurité qui est reconnue mondialement. Près de 10 000 personnes détiennent ce titre à travers le monde. Pour réussir l'examen menant à cette certification, les gens doivent maîtriser différents sujets dont l'analyse de risques, l'audit de sécurité et la sécurité physique.

La certification 'Physical Security Professional' (PSP) est aussi offerte par ASIS International. Le professionnel certifié PSP est mieux outillé pour évaluer la sécurité physique d'une organisation et pour faire des choix en ce qui a trait aux mesures de sécurité physique et à l'implantation de ces dernières.

Lors de notre collecte des données, nous avons rencontré trois experts qui avaient la certification CPP. Un autre avait obtenu l'Attestation Professionnelle en Gestion de la Sécurité Privée (APGSP) offerte par le Collège André-Grasset. L'APGSP était donnée en collaboration avec ASIS International et elle avait, entre autres, l'objectif de préparer les experts pour l'examen menant à la certification CPP. Pendant notre entretien avec James, ce dernier s'est référé à ses notes de l'APGSP pour nous expliquer des concepts reliés à l'audit de sécurité et à l'analyse de risques.

4.1.2 Littérature et publications

Plusieurs ouvrages ont été publiés par ou avec la collaboration de l'ASIS International. La majorité de ces ouvrages sont disponibles à partir du site Internet de la société, parfois même gratuitement (exemple : General Security Risk Assessment Guideline). En 2003, ASIS Int. a aussi fait une transaction importante en acquérant le 'Protection

of Assets Manual' (POA). La première édition de ce manuel remonte à 1974 et depuis sa création il a été mis à jour et revu à maintes reprises. Encore aujourd'hui, il s'agit d'un manuel très important en matière de protection des actifs et il est considéré comme une 'bible' par plusieurs experts. Il peut s'avérer très utile pour eux lorsqu'ils ont à réaliser des audits de sécurité. ASIS Int. publie aussi une revue mensuelle portant le nom de 'Security Management'. Les membres ont droit à quelques numéros qui leur sont envoyés gratuitement par la poste. Ceux qui le désirent peuvent aussi recevoir via leur courrier électronique la revue de presse quotidienne 'Security Management Daily'.

Beaucoup de livres que nous avons consultés ont été écrits par des membres de l'ASIS Int. et publiés en collaboration avec l'organisation. Plusieurs de ces ouvrages ont été écrits par des experts détenant la certification CPP ou PSP. Nous pensons aux livres de James F. Broder, de James L. Schaub, de Ken D. Biery, de Lawrence J. Fennely, de Mary Lynn Garcia, de Charles A. Sennewald, de Robert J. Fisher et de Gion Green. Il est possible de se les procurer en passant par le site Internet de l'ASIS ou en les commandant à partir du catalogue 'ASIS Bookstore' envoyé par la poste aux membres. Certains ont fait l'objet de critiques dans les numéros du 'Security Management'.

La majorité des experts que nous avons rencontrés durant la collecte de nos données utilisent ces ouvrages et s'y réfèrent quand ils ont à faire un audit de sécurité pour une organisation. Sébastien se base en grande partie sur les concepts développés pour la certification CPP, les différents livres d'ASIS et sur le POA pour développer son guide d'audit. Simon quant à lui s'aide des différentes méthodes retrouvées dans ces livres lorsqu'il audite une organisation et compare ce qu'il observe avec les façons de faire rapportées dans ces écrits.

Quelques entretiens se sont déroulés dans les bureaux des experts et nous avons constaté que plusieurs livres sur lesquels nous nous sommes basés pour faire notre recension des écrits se retrouvaient dans leur bibliothèque. James, Sylvio et Sébastien avaient quelques ouvrages à portée de la main. Les deux ouvrages qui ont été le plus

mentionnés par les experts sont le POA ainsi que le livre 'Risk Analysis and the Security Survey' de J. F. Broder que James considère comme étant une excellente référence en matière d'audit de sécurité.

4.1.3 Activités ASIS

Chaque année, il se tient un gros événement à Las Vegas. Il s'agit du séminaire/exposition organisé par ASIS International. Des membres provenant de différents pays se réunissent pour discuter de sécurité. Des forums virtuels sont aussi organisés à tous les mois et il est possible d'y assister via les différents chapitres de l'ASIS à travers le monde (Chapitre 196, Montréal).

En plus des forums virtuels, le chapitre de Montréal offre des soirées-conférences portant sur différents sujets du domaine de la sécurité. En février 2007, une soirée 'Comment faire' a porté sur le relevé de sécurité, sur l'analyse de risques et l'analyse d'impact d'affaires. Cette soirée a suscité beaucoup d'intérêt chez les membres puisque plusieurs personnes s'y sont présentées. L'auditoire était attentif et des gens prenaient des notes. Cela démontre l'intérêt qu'ils ont pour ces sujets.

4.1.4 Impact de l'organisation ASIS sur nos données

À notre grande surprise, nous avons rapidement pris conscience du fait que plusieurs experts de Montréal avaient adopté une méthode très similaire à celle développée par les membres de l'ASIS provenant des États-Unis. En effet, si nous comparons la méthodologie des experts de Montréal avec les cinq grandes étapes exposées dans la recension des écrits, nous y trouvons beaucoup de similitudes. Certains experts rencontrés proposent d'ailleurs une démarche quasi identique à celle décrite dans la recension des écrits. Il y a toutefois une remarque importante à faire à ce sujet. Si plusieurs experts utilisent abondamment la littérature spécialisée, il y en a moins qui s'inspirent des théories et des concepts développés en criminologie pour analyser la sécurité. La méthodologie est très similaire pour l'ensemble du projet, mais diffère

lorsque vient le temps de faire l'analyse des données recueillies sur le terrain. Nous aborderons cette question ultérieurement dans le mémoire.

Considérant que 12 des 16 experts rencontrés avaient un lien plus ou moins important avec le chapitre 196 de Montréal, il ne faut pas se surprendre de constater que les propos de plusieurs experts se rapprochent beaucoup de ce que nous avons lu tout au long de la recension des écrits. Ils ont accès à différentes ressources et les utilisent quand vient le temps de faire un audit de sécurité d'une organisation.

Sébastien affirme que le CPP permet à l'expert d'acquérir une base solide en sécurité et que cette accréditation est reconnue internationalement. Il avoue qu'il n'invente rien et qu'il s'inspire de ces concepts et de ces standards tout en les adaptant à l'entreprise pour laquelle il travaille. Il constate que le Québec est en retard si nous le comparons avec les États-Unis et avec l'Ouest canadien[2]. Selon lui, les experts d'ici devraient davantage être ouverts aux normes de l'ASIS et du CPP. Le fait d'être membre de cette organisation lui est bénéfique puisqu'il profite de l'échange d'informations et de trucs avec les autres gestionnaires en sécurité de la région.

4.2 Terminologie

Le terme 'security survey' ne semble pas avoir fait l'objet d'une traduction en français. Il semble y avoir une confusion concernant la terminologie francophone pour décrire le 'security survey'. Nous avons répertorié plusieurs termes pour décrire ce projet : audit de sécurité, inspection de sécurité, étude de sécurité, analyse de risques, analyse de besoins, diagnostic de sécurité et visite de sûreté. Les experts semblent utiliser différentes expressions pour décrire le même exercice qui consiste à faire l'examen méthodique d'une organisation ou d'un site dans le but d'identifier ses risques, ses vulnérabilités et les faiblesses de ses protections existantes, de statuer sur son niveau de sécurité et de recommander des solutions aux problèmes identifiés. Il nous apparaît

[2] En date du 10 septembre 2007 : 164 membres au Québec, 223 en Colombie-Britannique, 318 en Alberta, 707 en Ontario et en date du 2 août 2007 : 2702 membres en Californie, 1519 en Floride.

important d'analyser les différents termes désignant le 'security survey' et d'en retenir un qui sera privilégié dans notre recherche.

Au début de notre recherche, nous avions opté pour le terme 'inspection de sécurité'. Nous croyions à ce moment qu'il décrivait correctement ce projet et qu'il représentait la meilleure traduction du terme 'security survey' utilisée par les experts anglophones. Nous avons utilisé ce terme au moment de commencer notre collecte des données ainsi que pour approcher plusieurs experts afin d'obtenir une rencontre avec eux.

Nous avons rapidement compris que les gens rencontrés n'utilisent pas l'expression 'inspection de sécurité' et qu'ils ont recours à d'autres termes pour nommer notre projet. Parmi les experts interviewés, seule Karine utilise 'inspection de sécurité' pour nommer les projets qui consistent essentiellement à vérifier le bon fonctionnement des équipements de sécurité sur ses sites. Nous avons été surpris de constater que plusieurs expressions différentes pouvaient être utilisées pour décrire le même type de projet de sécurité. Nous en avons répertorié huit différentes : étude de sécurité, visite de sûreté, analyse de risques et de menaces, analyse des besoins, évaluation des besoins, enquête de sécurité, évaluation de sécurité et audit de sécurité. Dans le tableau 1, nous attribuons à chaque expert le terme qu'il utilise pour désigner ce que nous entendons par audit de sécurité.

Tableau 1 : Terminologie utilisée par les experts

Termes	Experts
Étude de sécurité	James, Myriam et Édouard
Visite de sûreté	Valérie, Gérald
Analyse de risques et de menaces	Simon, Pierre et Dimitri
Analyse des besoins	Cynthia
Évaluation des besoins	Karine
Enquête de sécurité	Peter
Évaluation de sécurité	Carol
Audit de sécurité	Ralph, Sébastien et Sylvio

Bien que nous ayons attribué un seul terme à chaque expert, il ne faut pas interpréter ce tableau en pensant qu'ils se limitent tous à une seule expression et qu'ils n'utilisent pas les autres. Certains experts utilisent plusieurs de ces termes pour définir l'audit de sécurité tel que nous l'entendons. Sébastien par exemple utilise à la fois les expressions étude de sécurité, inspection de sécurité et audit de sécurité pour définir le même projet. Il ne fait pas de distinction entre ces termes et pour lui ils se réfèrent au même processus. Il a toutefois une préférence pour le mot 'audit' et c'est ce qu'il utilise dans son entreprise.

D'autres experts utilisent plusieurs de ces expressions, mais font des distinctions claires entre celles-ci. James utilise 'étude de sécurité' pour nommer le projet que nous appelons 'audit de sécurité'. Même si pour lui l'audit est très similaire à l'étude, il fait une distinction entre les deux. Toujours selon James, pour réaliser un audit, il faut que la sécurité de l'organisation soit évaluée en fonction d'une norme établie. Édouard utilise aussi le terme audit lorsqu'il doit faire une vérification plus approfondie de la sécurité d'une organisation. Pour lui, le projet est un audit si l'expert vérifie et valide le bon fonctionnement des équipements de sécurité trouvés dans l'organisation. Les étapes de validation et de vérification ne sont pas faites, selon lui, dans une étude normale. Édouard donne l'exemple suivant pour illustrer ses propos : l'étude de

sécurité permet d'identifier la présence d'un système d'alarme alors que l'audit permet en plus de valider si le système fonctionne bien en testant par exemple le temps de réponse à une alarme.

4.2.1 Inspection de sécurité

Puisque nous avons approché les experts à l'aide d'une terminologie qu'ils n'utilisent pas, la majorité des personnes interviewées ont commencé leur entretien en proposant un terme pour remplacer l'expression 'inspection de sécurité' et nous ont expliqué pourquoi. Dès les premières minutes de l'entretien avec Édouard, il affirme trouver le terme inspection un peu trop technique. Valérie pour sa part mentionne qu'elle préfère remplacer le mot 'inspection' par 'visite' qui, selon elle, a une connotation moins négative.

Les deux personnes qui utilisent l'expression 'inspection de sécurité' font référence à des projets qui différent de ce à quoi nous nous attendions. Pour Karine, il s'agit d'inspections très techniques qui sont effectuées dans les différents bureaux de son organisation. Lorsqu'elle procède à une inspection, elle se rend dans un bureau durant les heures de fermeture et effectue une série de tests pour vérifier le bon fonctionnement des équipements en place. Par exemple, elle teste les détecteurs de mouvement, vérifie les alarmes avec la centrale, inspecte les instincteurs et vérifie qu'il n'y a pas d'élément qui empêche le matériel de bien fonctionner. Normalement, chaque site est inspecté à tous les six mois. Karine réalise aussi des évaluations de besoins pour ses bureaux. Il s'agit d'évaluations qui sont faites pour les nouveaux sites ou ceux où la sécurité est à revoir. Elle évalue à ce moment les besoins relatifs à la sécurité en rencontrant les gestionnaires des sites et en visitant les lieux. Suite à cette évaluation, elle est mieux outillée pour déterminer les mesures qui doivent être implantées pour que les lieux soient sécuritaires. Ces évaluations de besoins ressemblent davantage à ce que nous nommons 'audit de sécurité'.

Quant à Ralph, lorsque nous lui demandons à quel intervalle les inspections sont faites, il nous répond que cet exercice est fait à toutes les heures par ses agents de sécurité. Nous comprenons dès cet instant que nous ne parlons pas du même type de projet et qu'il fait plutôt référence aux 'rondes' de sécurité conventionnelles en parlant des inspections de sécurité. Dans son entreprise, ils utilisent plutôt 'audit de sécurité' et Ralph a une liste de contrôle pour vérifier son site. Il remplit cette liste une fois par année.

4.2.2 Étude de sécurité

D'après James, en étudiant une entreprise, l'expert arpente cette dernière, recherche des faits et vise à prendre la mesure de l'entreprise. Selon lui, plusieurs experts dans le milieu de la sécurité francophone utilisent 'étude' :

> Dans le milieu présentement tout le monde s'entend à peu près pour dire une étude. Si tu parles d'une étude de sécurité à quelqu'un généralement... C'est ce que le monde utilise présentement (James).

Pour James, l'expression 'survey' peut être remplacé par le terme 'étude de sécurité'. Il est toutefois conscient que certains experts ne sont pas encore habitués aux termes et qu'il faudrait se pencher sur cette question pour trouver un mot qu'ils pourraient mieux comprendre et utiliser.

4.2.3 Visite de sécurité

Pour Carol et Sébastien, la visite de sécurité est faite au début d'un projet d'audit et a pour but de développer le mandat. Avant d'établir sa méthodologie, Carol fait cette visite pour connaître le site. Pour Sébastien, c'est la visite préliminaire où il s'assoit avec le directeur du site pour se présenter, rencontrer la direction et visiter sommairement les lieux afin de préparer son audit. Il fait cela pour « casser la glace ». De son côté, Sylvio entend par visite de sécurité les « spots check » qu'il effectue à ses

sites satellites pour « s'assurer qu'il n'y a pas de changement au niveau de la sécurité » (Sylvio).

Valérie quant à elle utilise l'expression 'visite de sûreté' pour parler du projet au grand complet, de l'arrivée sur le site jusqu'au dépôt du rapport.

4.2.4 Audit de sécurité

L'entreprise pour laquelle Sylvio travaille étant assujettie à plusieurs réglementations de la part des gouvernements et oeuvrant dans un « monde de conformité », ce dernier préfère utiliser 'audit de sécurité'. Pour lui, l'audit est un examen complet de l'entreprise :

> Un audit, on part à 4 et on regarde tout. Chaque poteau, chaque maillon, chaque trou dans la clôture, chaque caméra, chaque bout de fil. Il es-tu sécurisé? Il es-tu à la bonne place ? On va à 100 % (Sylvio).

Il ajoute que c'est un exercice plus rigoureux et plus complet qu'une inspection de sécurité. L'inspection étant une marche sur le site pour regarder ce qui va et ce qui ne va pas.

Sans vouloir dénigrer le mot 'inspection', Sébastien préfère parler d'audit de sécurité. Étant un nouvel employé au sein de l'entreprise, il tente tranquillement d'implanter ce terme dans son organisation. « C'est peut-être psychologique comme mot, mais c'est un mot qui allume plus » (Sébastien). Selon lui, ses patrons aiment bien ce terme et ils l'ont déjà adopté. Quand ils entendent 'audit' ils sont plus attentifs. Toutefois, il est souvent obligé de rectifier son vocabulaire auprès des directeurs des entrepôts qui sont audités. Quand il leur annonce qu'ils vont faire l'objet d'un audit, ces derniers semblent découragés et il est obligé de leur dire qu'il s'agit en fait d'une visite pour développer un programme de sécurité.

La réaction des directeurs avec lesquels Sébastien travaille reflète la crainte que les gens peuvent avoir lorsqu'ils sont sur le point d'être audités. Valérie semble avoir perçu cette crainte :

> On essaie tout le temps par exemple de ne pas avoir une connotation négative. Quand on va dans nos sites, si tu parles d'audit c'est trop, ça leur fait peur. On dit vraiment qu'on vient faire une visite de sûreté pour leur donner des conseils. Voir ce qu'il se passe. Parce que c'est tout le temps volontaire. Nous on y va à leur demande. On essaie de ne pas leur faire peur. Pour ne pas qu'il nous voit comme des méchants. Des audits ce serait vraiment pour punir, pour dire, pour voir vraiment, pour corriger obligatoirement. Et puis tu as ça à respecter. Tu as des fautes comme à l'école. Mais nous autres, ce n'est pas ça qu'on veut faire. On ne veut pas les mettre devant une situation qui les rend responsables s'ils ne le font pas. On veut les amener à volontairement vouloir le faire. On ne veut pas leur donner des coups. On veut vraiment les amener à contribuer avec nous autres. Mais l'audit nous on considère que c'est quand tu as des règles fixes à respecter. La police ou des réglementations. Il faut faire ça dans tant de jours, dans tant d'heures (elle fait des gestes de la main pour dicter des ordres). Nous autres on n'a pas de réglementation comme ça. On a des conseils. On a des procédures qui disent que vous devriez faire ça, mais c'est toujours basé sur le bon vouloir. C'est jamais... On ne fait pas de la dictature. C'est de la consultation (Valérie).

Pour ces raisons, Valérie a adopté une terminologie différente et utilise 'visite de sûreté' qui est plus neutre qu'audit de sécurité.

Comme il a été mentionné, d'autres experts vont utiliser 'audit de sécurité' lorsqu'ils ont à faire des projets de sécurité bien spécifiques. Par exemple, durant une évaluation de sécurité ou suite à cette dernière, Carol peut recommander d'auditer des éléments précis. Il peut s'agir d'un test d'intrusion visant à déjouer un gardien de sécurité et à entrer dans un endroit contrôlé sans avoir l'autorisation d'y accéder. Par ailleurs, Édouard peut recommander d'auditer en profondeur des éléments particuliers dans une organisation. Les autres éléments à l'étude ne seront pas analysés de façon aussi pointilleuse. Il avoue qu'il fait rarement des audits et qu'il s'agit d'une limite à laquelle il doit faire face. Pour sa part, James va nommer son projet 'audit de sécurité' s'il vérifie la sécurité d'un site en la comparant à une norme précise.

4.2.5 Confusion au niveau de la terminologie

Comme il a été démontré, quinze experts utilisent huit expressions différentes pour faire référence à des projets similaires. Ils ont opté pour leur propre expression pour présenter leur projet à leur organisation ou à leur client. Il n'y a pas de consensus quant au mot qui devrait être utilisé pour définir l'audit et il semble même y avoir une confusion quant aux termes qui sont utilisés. Par exemple, James mentionne que plusieurs spécialistes en sécurité mélangent l'étude de sécurité avec l'analyse de risques :

> Tu vas avoir beaucoup de monde qui vont mélanger une analyse de risques avec une étude de sécurité par contre. Il le mélange parce que l'analyse de risques est devenue très à la mode. [...] Faire une étude de sécurité ou faire une analyse de risques c'est deux choses qui se complètent, mais qui ne sont pas tout à fait pareilles. [...] Tout se chevauche. Mais en même temps, c'est des concepts qui sont très abstraits et des fois c'est difficile. Moi j'ai assez 'rushé' pour comprendre ça. Je n'étais pas capable de trouver les réponses. Quatre-vingts pour cent des spécialistes en sécurité, tu vas leur demander, et ils ne font pas la différence (James).

Cette information est difficile à capter et il faut travailler très fort sur ces concepts pour pouvoir faire la différence selon James. Il y a donc des spécialistes qui disent effectuer des analyses de risques alors qu'en réalité ils réalisent des études de sécurité.

Simon constate aussi au sein de son entreprise une difficulté à avoir leur propre lexique en sécurité sur lequel tous s'entendent afin d'utiliser les mêmes termes. Même au sein de son propre bureau, il a dû s'asseoir avec ses patrons et ses collègues afin qu'ils puissent s'entendre sur la définition des termes qu'ils utilisent dans leur quotidien. Ils ont échangé ensemble pour définir des termes comme 'risque', 'menace' et 'vulnérabilité'. Tous ne s'entendaient pas au départ sur les définitions à utiliser.

Les experts ne s'entendent pas sur la terminologie et utilisent plusieurs termes différents pour nommer le projet à l'étude. Cette situation sème la confusion à la fois chez les experts et chez les demandeurs qui ne savent plus à quoi s'attendre lorsqu'ils

parlent d'étude de sécurité, d'inspection de sécurité, d'évaluation des besoins ou encore d'audit de sécurité. Idéalement, un seul terme devrait être utilisé par tous pour décrire les examens méthodiques effectués dans les organisations.

Le terme 'audit de sécurité' a été retenu aux fins de cette recherche. Ce ne fut pas un choix facile à faire puisqu'il y avait toujours des avantages et des inconvénients rattachés à chacun des termes. L'expression 'audit de sécurité' nous paraît être un bon choix puisqu'il fait référence à un examen approfondi de l'organisation. À notre sens, l'examen doit avoir une certaine profondeur pour donner des résultats. Il nous paraît risqué de faire des inspections trop sommaires.

La plus grande problématique avec le terme 'audit' c'est qu'il est susceptible d'inquiéter les employés des organisations auditées comme l'on mentionné Valérie et Sébastien. Il est important d'évaluer la portée des mots utilisés et de bien présenter le projet aux intéressés. Il n'est pas à l'avantage de l'expert de se mettre à dos les employés et d'obtenir une mauvaise collaboration de leur part. Dans bien des cas, il a besoin de leur collaboration afin de collecter des données intéressantes. Cette ouverture et cette collaboration étant parfois difficiles à obtenir, l'expert doit mettre les chances de son côté afin de recueillir les informations désirées de la part des employés. Dans l'intérêt du projet, il sera parfois nécessaire de changer le terme 'audit' par un autre mot si nous anticipons qu'il aura une incidence négative.

Dans l'éventualité où l'étendue du mandat ne permette pas de réaliser un examen approfondi de l'organisation, le mot 'audit' peut être remplacé par un autre terme. Il ne faudrait pas laisser sous-entendre au demandeur que son organisation va faire l'objet d'une étude en profondeur si ce n'est pas le cas. Quelques gestionnaires s'attendent à ce que l'expert aille au « fond des choses » s'il audite leur entreprise (Édouard).

Même si nous considérons qu'une terminologie partagée et connue de tous serait l'idéal, nous croyons qu'il peut y avoir un assouplissement à ce niveau. L'aspect le plus important demeure le fait que le demandeur ainsi que toutes les autres personnes

impliquées connaissent et comprennent bien les paramètres du projet. Le mandat doit être clair et cela peu importe la terminologie qui sera adoptée.

4.2.6 Sécurité ou sûreté ?

Dans l'expression 'audit de sécurité', il n'y a pas que le premier mot qui sème la confusion. Le dernier mot est aussi problématique puisque certains semblent hésiter entre 'sécurité' et 'sûreté'. D'autres utilisent tout simplement 'besoins'. Valérie travaille pour l'équipe qui s'occupe de la sûreté de l'entreprise. Elle voit une différence entre 'sécurité' et 'sûreté'. Selon elle, et comme le proposent Geiben et Nasset (1998), la sécurité est davantage reliée à la 'santé et sécurité au travail'. Cette distinction n'a pas été faite dans l'entreprise de Sébastien. Il fait partie de l'équipe de 'santé et sécurité au travail' bien qu'il affirme gérer la sûreté de l'entreprise en s'occupant, par exemple, de la sécurité physique des lieux, de la protection du personnel (excluant les accidents) et des enquêtes. Sébastien a la même vision que Valérie et travaille pour que la sûreté dans son entreprise soit une entité à part entière. Les experts veulent se détacher du mandat de 'santé et sécurité au travail' et faire connaître leurs véritables fonctions.

Par ailleurs, Simon a remarqué que les gens rencontrés dans les usines ont tendance à croire qu'il s'occupe du volet 'santé et de sécurité au travail'. Les travailleurs ont été conscientisés à porter l'équipement de sécurité fourni par l'employeur. Quand Simon se présente dans ce type d'entreprise, les employés ont souvent le réflexe de dire qu'ils portent correctement leur équipement :

> Quand tu es dans le milieu industriel, ils ne comprennent pas. Tu dis je suis ici pour la sécurité et je me fais répondre : 'j'ai mes bottes!' (les gens lui répondent avec un ton ennuyé) (Simon).

Simon doit donc expliquer aux travailleurs les raisons pour lesquelles il va les rencontrer et faire la distinction entre son mandat et celui des gens qui s'occupent de la 'santé et sécurité au travail'. Les personnes sur le terrain ne sont pas habituées à ce

genre de mandat de sécurité et les experts ont souvent à expliquer leur rôle et le but du projet.

4.3 Audit : projet en développement

Lorsque nous allions rencontrer des experts travaillant pour des services de sécurité interne d'entreprises multinationales, nous nous attendions à rencontrer des gens chez qui l'audit était un projet implanté depuis plusieurs années. À notre grande surprise, ce ne fut pas toujours le cas. Par exemple, le poste de 'chef sûreté' dans l'entreprise de James venait d'être créé et l'audit de sécurité était un nouveau projet qu'il venait à peine d'implanter dans son organisation. De son côté, Sébastien nous a confié qu'il est un nouvel employé pour son organisation et qu'il commence à effectuer des audits sur ses sites. Ces projets n'étaient pas faits par son prédécesseur.

Une surprise fut notre rencontre avec Valérie qui travaille pour une grande multinationale. L'équipe de sûreté est implantée depuis longtemps dans cette entreprise. Valérie venait de mettre en place un programme informatique afin d'aider les personnes chargées de faire les audits des sites à travers le monde. Il s'agit d'une nouvelle application dans cette entreprise. Au moment de l'entretien, environ 25 pour cent des sites avaient été audités à l'aide de ce logiciel. Les autres allaient être inspectés dans les années à venir. Nous avons aussi appris que seulement 10 % des sites avaient un responsable de sûreté sur place.

4.4 Audit de sécurité dans un contexte général

La façon la plus simple de percevoir l'audit de sécurité est de se limiter à dire qu'il s'agit de la démarche effectuée sur le terrain pour recueillir les données et pour faire le relevé des vulnérabilités d'une entreprise. Il s'agit d'un outil qui permet de faire un bon relevé des forces et des faiblesses de l'entreprise. Cette façon de voir l'audit est tout à fait juste, mais il ne faut pas oublier de situer cette démarche sur le terrain dans son contexte. Cette cueillette de données s'inscrit toujours dans un projet d'audit de

sécurité plus large. La majorité des experts rencontrés proposent des étapes à suivre pour effectuer un audit de sécurité : préparation, cueillette des données, analyse de ces données et finalement le rapport. Ces étapes seront détaillées ultérieurement dans le mémoire.

Pour la majorité, l'audit se termine une fois que le rapport est déposé et expliqué au demandeur. Toutes les étapes qui suivent le dépôt du rapport ne sont plus considérées dans l'audit. Plusieurs autres projets peuvent découler du rapport, mais ils ne sont pas considérés comme faisant partie de l'audit. Dans ses rapports, Simon inscrit des recommandations générales à ses clients. Il s'agit de recommandations qui ne sont pas suffisamment détaillées pour que le client puisse les appliquer par lui-même. Par exemple, en auditant l'un de ses clients, Simon a constaté qu'il y avait des lacunes importantes dans les mesures et les procédures d'urgence de l'organisation. Dans son rapport, il a donc recommandé de revoir ces mesures sans expliquer au client comment faire. Si ce dernier est intéressé à appliquer cette recommandation, l'équipe de Simon est disposée à retourner sur place afin de lui proposer un projet pour parfaire les mesures d'urgence. Pour les experts, l'implantation des recommandations est une étape indépendante qui suit l'audit.

D'autres projets ou sous-projets peuvent être réalisés durant ou suite à l'audit. Par exemple, il arrive parfois que Carol et Édouard recommandent des vérifications très pointues sur des éléments spécifiques (exemples : système informatique, système d'alarme, comptabilité). Ces vérifications en profondeur peuvent être faites en même temps que l'audit ou être recommandées dans le rapport final.

Une autre action qui peut être réalisée durant l'audit est une analyse des risques de l'organisation. Bien qu'une forme d'analyse des risques soit souvent faite par des experts avant de procéder aux recommandations, elle ne sera pas toujours présentée au client comme un produit :

> On ne va pas oublier de faire l'évaluation des risques, mais on ne va pas nécessairement en faire un produit pour le client (Édouard).

Étant limités en temps et en argent, les experts ne sont pas toujours en mesure de faire une analyse de risques en profondeur. Lorsqu'ils agissent comme consultants, James et Édouard ne peuvent pas toujours se permettre de faire un audit accompagné d'une analyse très rigoureuse puisque souvent les mandats ne le permettent pas.

4.5 Audit : projet circonscrit ou exercice continu

Les experts s'entendent pour dire qu'un audit n'est pas un exercice qui est fait une seule fois dans une organisation. Il s'agit d'un travail qui doit être répété en fonction d'un intervalle qui va varier selon le type d'organisation et en fonction d'autres facteurs à considérer. Les entreprises dynamiques qui subissent des changements et qui ont des opérations compliquées doivent être auditées plus régulièrement que les autres. Il n'est pas certain que des mesures efficaces en place à un moment donné vont demeurer efficaces suite à des changements dans l'organisation. Les changements apportent souvent de nouvelles vulnérabilités. Il est donc important pour un expert de revoir la sécurité avec le temps et de refaire des analyses pour déterminer si une organisation est toujours sécuritaire.

Une organisation qui a négligé sa sécurité peut être auditée plus fréquemment durant une période de temps pour régler ses problèmes sécuritaires. Par exemple, James a été engagé par une entreprise importante qui n'avait pas de 'chef sûreté' dans ses établissements de Montréal. La réalisation d'un audit de sécurité a été l'une des premières choses qu'il a eu à effectuer et il n'a pas pu la réaliser en profondeur. Il s'est contenté de faire un relevé général des problèmes et de gérer ceux qui étaient prioritaires. Il a mentionné que d'autres audits seront effectués à court terme pour analyser son entreprise plus en profondeur. Sébastien est aussi arrivé dans une multinationale qui n'était pas habituée à se faire auditer par le chef sûreté. Il a pris beaucoup de temps pour faire l'inspection de ses différents sites et les a analysés en profondeur. Contrairement à James, il nous dit que les audits qui vont suivre seront plus faciles et moins longs à réaliser ayant déjà fait beaucoup de travail initialement.

Il semble impossible de déterminer l'intervalle idéal qui devrait séparer deux projets d'audit. Il y a trop de facteurs qui vont jouer sur cette période de temps. Pour James, c'est un bon exercice à faire une fois par année ou aux deux ans s'il n'y a pas trop de changements dans l'organisation. Sébastien semble déterminé à faire les inspections de ses sites à chaque année. Karine vérifie le bon fonctionnement des systèmes de ses sites aux six mois. Ayant plusieurs sites à gérer, l'intervalle peut s'étendre jusqu'à cinq ans pour Valérie. Elle envisage éventuellement de permettre à ses sites de s'autoévaluer à l'aide d'un guide qu'elle pourrait mettre à leur disposition. Cette autoévaluation pourrait être faite à chaque année.

Contrairement aux gens qui ont à gérer plusieurs sites souvent éloignés, certains experts bénéficient d'une proximité avec les établissements qu'ils ont à gérer. Cela leur permet d'acquérir une connaissance importante sur ceux-ci et sur les opérations qui s'y déroulent. Sans être continuellement en audit, ils peuvent plus facilement être à jour vis-à-vis les changements dans l'organisation et y ajuster la sécurité en conséquence. Lorsqu'un audit doit être réalisé, il est plus facile pour eux de se prêter à cet exercice. Sylvio est régulièrement audité et dit avoir une excellente connaissance de son environnement. C'est la même réalité pour Sébastien dont le bureau est situé sur le site le plus important de son entreprise. Il y fait régulièrement des inspections informelles pour vérifier les faiblesses et tenter de les corriger sur le moment.

Même les experts qui ont un seul ou peu de sites à gérer doivent effectuer des projets d'audits. James, Sylvio, Sébastien et Karine ont remarqué que plusieurs petits changements peuvent s'opérer dans une organisation à l'insu de l'expert. À certains moments, ils doivent eux aussi prendre du recul et se questionner :

> Si tu as oublié de te questionner pendant un mois, arrêtes et prends le temps de te questionner s'il n'y a pas eu des changements dans ton organisation. Le plus grand danger de la sécurité, c'est la complaisance. Il n'y a rien de plus facile que de s'asseoir à l'arrière d'un bureau et de dire : 'bien, j'ai le système et je ne touche plus à ça'. Et là tu te laisses aller et la première chose que tu sais, bien tu te plantes (Sylvio).

Il est donc important de s'arrêter pour analyser la sécurité d'une organisation. L'audit est un outil pour réaliser cet exercice. James a aussi constaté qu'il peut être difficile de délaisser les opérations, les autres projets et les problèmes quotidiens pour se pencher sur l'analyse globale de la sécurité de l'organisation. Étant occupés à autre chose, les experts ne sont pas toujours en mesure de consacrer du temps pour auditer leur organisation.

4.6 La demande des audits de sécurité

Idéalement, toutes les grosses organisations doivent être auditées (James). Les raisons qui expliquent la demande d'un audit de sécurité dépendent souvent du type d'organisation et de ses caractéristiques (Édouard). Étant assujetties à des normes, les organisations publiques ou parapubliques agissent de façon proactive et demandent les audits avant la survenance des problèmes. À l'autre extrême, les PME sont plus réactives et vont attendre qu'il y ait un réel problème avant de prendre une action. Certaines entreprises vont même attendre qu'il y ait plusieurs problèmes ou une problématique grave avant de réagir (Édouard). Leurs priorités sont davantage orientées vers le profit et les opérations.

4.6.1 Raisons qui expliquent la demande

Quelques experts nous ont exposé des raisons expliquant la réalisation d'un audit de sécurité dans une organisation. La direction peut demander l'avis d'un expert ou une opinion indépendante d'un consultant externe avant d'investir de l'argent dans la sécurité. L'audit peut être un exercice cyclique réalisé selon un échéancier prédéterminé. Le désir de rencontrer certaines normes ou d'être accréditées à des programmes peut amener certaines organisations à être auditées. Par exemple, le programme 'Customs-Trade Partnership Against Terrorism' (C-TPAT) incite plusieurs entreprises qui font du commerce avec les États-Unis à réaliser des audits pour améliorer leur sécurité afin d'obtenir leur accréditation. Un relevé de sécurité complet a été développé pour aider les gens à se conformer aux exigences C-TPAT. Il est

disponible sur Internet moyennant une somme d'argent. Plusieurs entreprises montréalaises font appel à des experts qui vont les aider à obtenir la certification qui leur permettra de bénéficier des différents avantages rattachés à son obtention (exemples : passage plus rapide à la frontière américaine, moins d'inspections effectuées sur la marchandise).

4.6.2 Problématiques

Durant nos entretiens, plusieurs experts ont mentionné que des audits sont effectués suite à des problèmes rencontrés par les organisations. Le demandeur peut connaître la nature de son problème dès le départ et demander un audit dans le but de trouver des solutions. D'autres fois, il constate la présence d'un problème sans toutefois être capable de l'identifier. Il demande alors l'aide d'un expert pour le trouver et le résoudre. Finalement, la problématique peut être soulevée par l'expert. Certains problèmes peuvent être difficiles à cerner par une personne qui n'a pas beaucoup de connaissances sur la sécurité. D'autres ne sont pas soulevés à cause de la négligence ou de l'insouciance des gens qui travaillent pour l'organisation. Selon les experts, l'audit permet d'analyser les problématiques et d'éviter de chercher des solutions avant de penser aux causes qui expliquent la présence de ces problèmes. Par exemple, un problème de vols internes ne sera pas nécessairement réglé en installant des systèmes de contrôle d'accès si les employés fautifs détiennent une carte d'accès.

4.6.3 Investissement en sécurité

Quand vient le temps d'investir dans la sécurité, les gestionnaires peuvent procéder de différentes façons pour déterminer les fournisseurs qui feront le travail et pour décider des équipements à installer. Une façon de faire qui est très répandue est le système par soumissions. Voulant investir dans la sécurité, plusieurs gestionnaires appellent deux ou trois fournisseurs et demandent des soumissions. Celui qui dépose la soumission la plus intéressante obtient le contrat de sécurité et installe les systèmes pour le client.

Le cas Ralphy

Durant notre collecte des données, nous avons rencontré Ralph. Il est le responsable de la sécurité sur l'un des sites de l'entreprise Ralphy. Les principales opérations qui se déroulent sur le site géré par Ralph sont l'entreposage et la distribution des produits de l'entreprise Ralphy. Ralph est un administrateur n'ayant aucune formation en sécurité et le mandat de sécurité lui a été donné par intérêt. Parmi les mandats qui lui sont conférés, c'est celui de la sécurité dans lequel il investit le moins de travail. Une autre personne gère la sécurité de tous les sites en Amérique du Nord. Bien que Ralph puisse compter sur l'expertise de celle-ci, il dit la contacter très rarement.

À chaque année, Ralph remplit un 'self-audit' pour évaluer la sécurité sur son site. Ce formulaire standardisé en anglais est fourni par une équipe établie aux États-Unis. À chaque année, il le complète et le renvoie à cette équipe. Ralph dit connaître suffisamment son site et être en mesure de compléter le 'self-audit' à partir de son bureau.

Lorsque nous lui demandons si son site subit des problèmes de sécurité, il répond qu'il s'est fait voler un conteneur l'an dernier. Ralph est conscient que ses employés volent de petits objets sporadiquement sans connaître l'importance de tous ces vols combinés. Selon lui, il est trop difficile de contrôler ces petits vols et d'avoir le contrôle de son inventaire. Les produits étant fabriqués sur un autre site, les pertes peuvent être constatées dès la réception de la marchandise. Il est difficile pour lui de déterminer la cause des pertes et il avoue qu'il ne s'agit pas d'un problème grave pour lui. Pour éviter les abus, il dit faire des fouilles aléatoires.

Au moment où nous nous sommes présentés sur les lieux, nous avons constaté que de gros travaux étaient en cours sur le site. Une nouvelle structure était en construction et allait éventuellement se joindre à l'entrepôt déjà existant. Avec cet ajout, la capacité d'entreposage allait doubler. Ralph a été la personne responsable d'implanter les mesures de sécurité dans ce nouveau secteur. Pour réaliser son mandat, il a fait appel à

trois fournisseurs d'équipements de sécurité et a retenu les services de l'entreprise qui a soumissionné le moins cher. Il n'a pas fait appel à un conseiller en sécurité jugeant que les gens des services-conseils ne font que rajouter 10 à 15 pour cent de frais. Il a estimé être capable d'évaluer lui-même les besoins en matière de sécurité. Pour Ralph, « la sécurité n'est pas une science infuse ». Sa compagnie a une politique du moindre coût et il dit vouloir éviter les dépenses inutiles.

Pour sécuriser son site, Ralph a fait installer des caméras de sécurité et a perfectionné le contrôle de ses accès. Il a aussi ajouté une guérite opérée par un agent de sécurité pour contrôler l'accès à sa cour. De tous les sites de l'entreprise Ralphy, il est le premier à faire installer ce système de guérite.

Le cas de l'entrepôt Ralphy n'est pas unique. Il s'agit d'une pratique qui est largement répandue. Les gestionnaires décident de ne pas faire appel à un expert lorsque vient le temps d'investir dans la sécurité et tentent de déterminer leurs besoins par eux-mêmes. Carol a rencontré des gens qui ne savaient pas qu'il y avait des professionnels qui se spécialisent dans les services-conseils dans le domaine de la sécurité. Certains vont tout de même arriver à sécuriser leur organisation convenablement alors que d'autres ne réussiront pas. Il est parfois inquiétant de penser que la sécurité d'une organisation puisse être entre les mains d'un fournisseur ayant réussi à soumissionner le moins cher (James). Selon James, il ne devrait pas avoir aucun programme de sécurité de développé sans avoir fait au préalable un audit de sécurité.

Dimitri a installé des dispositifs de sécurité électroniques pendant un certain temps et il fait maintenant de la consultation. Il a constaté que ses clients lui demandaient souvent d'installer des dispositifs qui ne comblaient pas leurs besoins et qui ne donnaient pas de résultat. Il met en garde les entreprises et mentionne qu'il faut faire attention de ne pas installer des systèmes inutiles. Ce ne sont pas tous les fournisseurs qui vont informer leurs clients qu'ils sont sur le point d'implanter des systèmes plus ou moins adaptés à leurs besoins et la plupart vont procéder à l'installation. D'autres voient toujours les solutions comme étant technologiques :

> Mon expérience comme je vous l'ai dit tout à l'heure, moi je suis du domaine de la protection électronique et de l'installation de composantes électroniques. Je vous dirais qu'il faut faire attention à ces gens parce que la plupart du temps ils voient la solution comme étant technologique. Pour eux autres, un problème ça nécessite par exemple une caméra alors que des fois c'est autre chose (Dimitri).

Les experts rencontrés aiment donner des exemples de projets pour lesquels la solution finale n'a pas été un gros investissement d'argent et ni l'implantation de technologie. Dans ces cas, la solution était souvent un simple changement dans les procédures de l'organisation.

4.6.4 L'audit de sécurité et le programme de sécurité

L'audit de sécurité est un outil très pratique. C'est la base pour plusieurs autres projets :

> Pour moi l'inspection de sécurité ça s'inscrit plus dans un cadre général d'évaluation des risques et ultimement un programme de sécurité et programme de maîtrise des risques aussi (Édouard).

> Ce qui va tirer ton train, c'est ton étude. C'est ton étude de sécurité, ou ton inspection si tu aimes mieux, qui va être le ramassage d'informations. Lui va te permettre de faire l'analyse de risques. Il va te permettre de faire l'analyse d'impact d'affaires. Va te permettre de faire des recommandations. Pis ton wagon de queue c'est toujours tes recommandations (James).

Grâce aux informations qui sont recueillies lors de l'audit de sécurité, l'expert est en mesure de réaliser diverses analyses dont l'analyse de risques. Ce projet va aussi servir de base pour un éventuel programme de sécurité. Ce programme est très intéressant pour l'organisation, car il va aider le professionnel à réaliser une implantation cohérente et efficace des mesures de sécurité.

En connaissant l'organisation et en ayant fait un audit puis mis en place un programme de sécurité, l'expert est mieux outillé pour prendre des décisions quand vient le temps d'accepter ou de refuser d'implanter des contre-mesures :

> Moi je refuse à toutes les semaines. Je refuse d'installer des portes avec des contrôles d'accès à toutes les semaines. Les employés me demandent : 'ah! je veux une porte à telle place'. Non ! Pas besoin de ça. Il y a déjà quatre niveaux de sécurité pour se rendre chez vous et ça s'arrête là. Tu n'as pas besoin de plus que ça. Ça, on le fait parce qu'on a une excellente connaissance de notre environnement. On l'a tellement fait l'audit, on l'a tellement répété [...] Alors que moi les employés me demandent des caméras. Ils veulent toujours en rajouter et c'est moi qui suis obligé de dire non. Pour eux autres, si je les écoutais, les employés, il y aurait trois fois le nombre de caméras que j'ai sur le site présentement (Sylvio).

Il est important de ne pas faire de la sécurité à la pièce et d'éviter d'installer des systèmes aux endroits déjà suffisamment protégés. Sylvio n'est pas le seul expert qui a à refuser d'implanter des systèmes de sécurité demandés par ses employés :

> Souvent ils vont vouloir tout sécuriser. Si on les écoutait, il y aurait des lecteurs de cartes sur à peu près toutes les portes dans le bâtiment. Mais est-ce que ça vaut vraiment la peine ? On leur explique aussi c'est quoi la contrepartie d'un lecteur de cartes. [...] C'est bien beau leur dire, ils vont mettre des caméras partout. Mais la caméra, il faut qu'il y ait quelqu'un qui la regarde. Pis si on en a trop dans l'entreprise, bien on ne peut pas fournir à tout regarder. Ça ne règle pas tout une caméra (Karine).

L'une des tâches de Karine est de conscientiser les directeurs sur l'impact que peuvent avoir les systèmes sur les sites et sur les opérations. Elle connaît suffisamment les installations pour décider si les demandes sont justifiées ou non.

Les mesures doivent s'intégrer aux autres déjà en place. En arrivant dans son organisation, James s'est rendu compte qu'il y avait deux systèmes différents de télésurveillance. L'un d'eux était compatible avec ses graphiques informatiques et l'autre non. Cette incompatibilité complique son travail et il lui est plus difficile de visionner les images produites par ce second système.

Carol juge important que les solutions doivent s'intégrer à la culture de l'entreprise et être acceptées par les personnes qui travaillent pour l'organisation. Si l'expert ne tient pas compte de l'avis des travailleurs et implante des mesures qui ne sont pas acceptées par eux, et bien elles risquent d'être moins efficaces. Les travailleurs peuvent être tentés de contourner les systèmes et de ne pas les utiliser à bon escient.

Les experts doivent respecter les normes, les règlements et les lois applicables. Il s'avère risqué d'installer des caméras à des endroits où c'est proscrit par la loi (Carol). En tenant compte des caractéristiques du site, le professionnel évite d'installer de l'équipement inadéquat. Il n'est pas avantageux d'installer un système de contrôle d'accès sophistiqué et coûteux sur une porte ayant une structure déficiente. S'il est facile de briser le mur à côté de la porte et de débarrer cette dernière par l'intérieur, les contrôles d'accès ne servent plus à rien (James). Dans l'un de ses mandats, Carol a rencontré un président qui avait fait installer environ 35 caméras dans son usine. Les moniteurs et le système d'enregistrement se trouvaient dans son bureau où il consacrait au maximum 20 pour cent de son temps. Installés ainsi, les moniteurs n'étaient pratiquement jamais visionnés ce qui réduisait énormément l'efficacité de la télésurveillance dans cette usine.

N'ayant pas de plan de travail, il est plus probable d'investir dans des mesures de sécurité qui s'avèrent plus ou moins efficaces (James). Constatant que des problématiques demeurent après les investissements initiaux, d'autres sommes d'argent risquent d'être investies pour corriger la situation. Cet exercice peut être répété plusieurs fois pour finalement se rendre compte que trop d'argent et de temps ont été mis dans la sécurité qui n'est toujours pas adéquate. Il est préférable de faire une bonne analyse dès le départ pour ensuite développer un programme de sécurité mieux structuré, mieux organisé et plus efficace.

4.7 La préparation

Avant de se rendre sur le terrain pour entreprendre la cueillette des données, une préparation s'impose.

4.7.1 S'informer au sujet de l'organisation

Cette étape s'adresse surtout au consultant externe qui est appelé à faire un audit de sécurité pour un client qu'il ne connaît pas. Avant de se rendre chez le client, les experts s'informent au sujet de l'organisation et cherchent le maximum d'informations à son sujet. Par exemple, Simon situe le site dans son environnement et si possible visualise les photos satellites disponibles gratuitement sur plusieurs sites Internet. Cette recherche d'informations peut se faire par le biais d'Internet. En connaissant l'organisation, Peter et Cynthia ont constaté qu'il y a moins de surprises lors de la première rencontre avec le client et ça démontre un certain professionnalisme.

4.7.2 La finesse de l'expert

Quelques experts soulignent l'importance de porter une attention à la façon de présenter le projet au demandeur. Il est présenté de façon à créer une ouverture et un intérêt de la part du demandeur. Il ne doit pas craindre l'audit et doit comprendre l'apport positif qu'il aura sur l'organisation (Sébastien, Valérie). Cette approche est appliquée avec tous les employés avec lesquels l'expert doit interagir. Il développe des trucs pour présenter le projet de façon à ce qu'ils ne se sentent pas persécutés (Simon). Il explique aux gens qu'il rencontre qu'il n'est pas là pour attraper les personnes qui causent des problèmes à l'organisation. Il explique son mandat de façon à ce que les gens se sentent à l'aise. Cette attitude doit demeurer du premier contact avec le demandeur jusqu'au dépôt du rapport.

4.7.3 Rencontre avec la personne-ressource

Une rencontre a normalement lieu entre l'expert et la personne-ressource de l'organisation inspectée. Il s'agit souvent d'un gestionnaire dans l'entreprise (exemples : cadre, directeur de la sécurité, vérificateur interne, président). Le consultant externe rencontre le demandeur qui est porteur de l'audit dans son organisation. L'expert qui est employé par une organisation rencontre un supérieur pour développer un projet d'audit avec lui ou rencontre les personnes responsables des sites qui seront audités. Bien que le but et la nature de cette rencontre puissent varier, quelques actions précises sont accomplies dans la plupart des cas.

L'expert s'informe des raisons qui amènent une organisation à vouloir faire un audit de sécurité (James). Il cible aussi les attentes du demandeur. Il identifie les problématiques s'il y en a. Une évaluation des besoins est aussi effectuée (Karine).

Un élément important est délimité durant cette rencontre. Il s'agit du mandat. L'ampleur du projet est déterminée avec une personne ressource :

> Le succès du projet va dépendre de la combinaison entre les objectifs qu'on va avoir préalablement identifiés, les délais pour réaliser le projet, puis les moyens consentis par le client pour nous à l'interne (Édouard).

Les objectifs, les délais et les moyens nécessaires sont déterminés. Combien de temps est alloué ? Quels sont les moyens qui sont consentis pour réaliser le mandat ? Certains éléments devront être mis à la disposition de l'expert pour qu'il puisse mener à terme le mandat. Par exemple, la personne ressource devra préparer les documents qui lui sont requis (exemples : inventaire, plans des lieux, énoncé de mission de l'entreprise). L'expert doit être en mesure d'accéder à différents endroits sur le site et de rencontrer les employés. Idéalement, l'organisation se prépare à le recevoir. Les employés sont mis au courant de sa venue et connaissent la nature de son projet. Dans l'éventualité où la sécurité est testée, la direction est mise au courant des tests (Cynthia).

Les limites du mandat sont établies. Les éléments qui sont à l'étude et ceux qui ne le sont pas sont délimités. Par exemple, certains aspects qui ont trait à la 'santé et à la sécurité au travail', au système informatique ou aux mesures d'urgence peuvent ne pas être inclus dans le mandat. Il est important de clarifier ces points dès le départ avec le demandeur pour ne pas qu'il y ait d'ambiguïté. Le demandeur et l'expert s'entendent sur le mandat (Carol).

Suite à cette rencontre, l'expert prépare son audit de façon à respecter le mandat et les objectifs (Édouard). Les risques de ne pas rencontrer les attentes du demandeur sont beaucoup moins grands si le travail est basé sur un mandat clair. Dans l'éventualité où il est pertinent d'ajouter de nouveaux éléments au mandat, il est conseillé d'en avertir le demandeur afin d'obtenir son avis et son approbation (Cynthia).

L'élaboration du mandat avec le demandeur est une étape déterminante pour la suite du projet. C'est à ce moment que les délais et les moyens sont décidés. Il est important de bien conseiller la personne qui demande à ce que son organisation soit auditée. L'ampleur du mandat est ajustée afin que celui-ci réponde aux besoins de l'organisation à l'étude. Pour Dimitri et Édouard, l'objectif est de trouver un compromis entre le manque de rigueur et la recherche de la perfection. Plus le mandat est important, plus les délais et les moyens le seront aussi. Ainsi, les délais et les moyens consentis doivent être suffisants pour que l'expert mène à bien un audit de qualité, mais doivent être réduits autant que possible pour ne pas dilapider inutilement le capital de l'organisation.

Dans l'éventualité où l'expert s'aperçoit que le mandat octroyé est insuffisant pour les besoins de l'organisation, il avertit le demandeur que la qualité du travail risque d'être compromise. Il l'informe qu'il peut y avoir des avantages à investir un peu plus de temps ou d'argent. Manquant de temps ou de fonds, l'expert ne peut pas effectuer une cueillette de données exhaustive et une analyse rigoureuse par la suite. James juge qu'il est préférable d'investir un peu plus pour réaliser un relevé de sécurité qui permet d'obtenir un bon diagnostic et de faire par la suite les meilleures recommandations

possibles pour améliorer le niveau de sécurité d'une organisation. Les experts sont conscients qu'ils doivent travailler avec plusieurs contraintes.

Les relevés trop sommaires ou trop généraux ne permettront pas d'évaluer efficacement le niveau de sécurité d'une organisation. En ne faisant qu'un survol, l'expert risque de rater des éléments importants.

Certains experts inspectent des éléments rattachés à la 'santé et sécurité' au travail au moment où ils effectuent des audits de sécurité. Lorsqu'un mandat est donné pour optimiser le niveau de sécurité d'une organisation, il devrait être clair qu'il ne s'agit pas de vérifier l'aspect 'santé et sécurité' au travail. Il doit y avoir une distinction entre ce qui touche à la sûreté et ce qui relève de la 'santé et sécurité' des organisations. Il existe bel et bien une confusion à ce sujet et l'expert devrait faire comprendre au demandeur que cette question ne fait pas partie de son mandat. Dans l'éventualité où l'expert constate une négligence importante sur ce plan, il en informe les gestionnaires sans le mentionner dans son rapport. S'il en fait état dans le rapport, les gestionnaires peuvent penser que l'expert s'occupe aussi de la 'santé et sécurité' au travail alors que ce n'est pas le cas. Dans le pire des cas, les gestionnaires peuvent se questionner à savoir pourquoi l'expert a omis plusieurs autres aspects qui menacent la santé des employés. Le mandat doit être clair et si certains éléments de la 'santé et sécurité' doivent absolument être vérifiés, alors il doit y avoir une mention spéciale à cet effet.

4.7.4 Les raisons qui limitent le mandat

L'expert et le demandeur développent toujours le mandat en tenant compte de certaines limites. Les moyens et les délais que peuvent consentir les organisations ne sont pas infinis :

> Disons que l'inspection de sécurité des fois il faut savoir tourner les coins ronds ou prendre des raccourcis pour la réaliser, justement parce que les moyens et les délais consentis ne sont pas à la hauteur de ce qu'on voudrait réellement faire si on était très puriste (Édouard).

Les experts ajustent l'audit en fonction des limites qui leur sont imposées. La limite monétaire est celle qui a été le plus mentionnée par les interviewés.

Dans certaines organisations, des départements ne souhaitent pas voir arriver un expert en sécurité dans leur champ d'expertise. James a eu des problèmes avec les gens qui s'occupent de l'informatique et avec l'équipe qui s'occupe de la 'santé et sécurité au travail'. Ces personnes ne voulaient pas le voir s'occuper des éléments qui touchaient à leur expertise :

> L'informatique c'est un petit secteur sensible. Ils n'aiment pas qu'on joue sur leur terrain. [...] À la seconde que j'ai soulevé ces points-là, nos services informatiques sont allés se dépêcher d'aller faire enlever cette partie de ma description de tâche. [...] Ils sont allés faire des crises pour faire enlever de ma description de tâche : document, IT network, electronic property. Alors pour l'instant, bien parfait, ça me fait moins de travail. Puis quand ça deviendra un risque qui est inacceptable pour l'entreprise, je vais m'en occuper. Il n'y a pas de problème. Ce sont des décisions d'entreprise et ça arrive souvent quand ton chef sûreté est à des niveaux moins hauts dans l'entreprise (James).

Certaines personnes n'ayant parfois pas les mêmes objectifs désirent ne pas partager leurs tâches. Cela nuit à la sécurité générale d'une organisation. À quoi bon avoir les meilleurs logiciels pour protéger son réseau informatique si la porte qui mène aux serveurs est vulnérable et qu'il est facile de pénétrer dans la salle dans le but de subtiliser quelques disques durs ? Selon Gérald et James, il faudra qu'il s'effectue une convergence afin d'être en mesure de sécuriser les organisations du périmètre jusqu'aux disques durs. Le chef sûreté occupe idéalement une position élevée dans la hiérarchie ce qui lui permet d'avoir un pouvoir décisionnel plus grand et de gérer la sécurité dans l'ensemble de l'organisation (ASIS International, 2004).

Les connaissances de l'expert peuvent ne pas couvrir certains champs d'expertise. Sébastien ne s'y connaît pas en sécurité informatique et compte sur l'équipe au sein de son organisation pour s'en occuper. Il est toutefois allé rencontrer un responsable de la sécurité informatique pour lui poser des questions. Pour certains contrats, Simon fait appel à des partenaires d'affaires afin d'auditer des systèmes plus techniques

(télésurveillance, contrôles d'accès, biométrie). Son partenaire fait alors une visite des lieux dans le but d'auditer ces systèmes et lui remet un rapport. Par la suite, Simon intègre à son rapport les constats et les recommandations de son partenaire. Édouard procède aussi de cette façon. Cynthia a eu connaissance que des gens auditent des éléments pour lesquels ils n'ont pas les compétences requises pour faire un bon travail et elle déplore cette situation. Il n'est pas professionnel, voire dangereux, de travailler de cette façon (Cynthia).

Une autre contrainte peut venir du fait que le demandeur ne veut pas que la réalisation de l'audit soit connue des employés, mais bien qu'elle soit faite de façon discrète (Édouard). Une telle situation limite grandement les manœuvres de l'expert.

4.7.5 Cibler les priorités

Lorsqu'il est limité dans ses démarches, l'auditeur ne peut pas inspecter tous les éléments de l'organisation avec la même profondeur. Le défi à ce niveau est de déterminer les éléments qui seront exclus, audités partiellement ou vérifiés rigoureusement. Pour ce faire, l'expert peut établir les actifs qui sont stratégiques pour l'organisation. Il tient alors compte de la mission de l'entreprise, des priorités organisationnelles et des priorités d'affaires :

> Le processus d'affaires va toujours découler de : on reçoit, on teste, on mélange, on compresse, on fabrique, on colt, on fait des bouteilles et ça sort dehors. En gros, la roue c'est ça que ça fait. Bien il faut que mon processus de sécurité supporte tout ça. Si ça ne supporte pas ça, ça a zéro priorité pour nous autres. Pas intéressant. (Sylvio).

L'auditeur examine les éléments qui ont un impact sur le processus d'affaires de l'entreprise. Plus un élément a de l'impact sur ce processus et plus l'expert lui accorde une attention particulière. Un actif qui est indispensable pour l'organisation est davantage audité, surtout si ce dernier est difficilement remplaçable :

> La machine numéro 3 dans l'usine qui fournit 50 % de la production de l'entreprise et qui a un coût de remplacement énorme et un délai de remplacement énorme. Cette machine-là si elle plante, peut-être qu'elle va avoir un impact beaucoup plus grand que trois autres machines réunies [...] Quels sont les actifs qui justement contribuent le plus à la réalisation de la mission de l'organisation ? [...] Puis parmi l'ensemble de ces services, quels sont les plus stratégiques ? Évidemment, il ne s'agit pas d'exclure d'actifs, mais c'est un peu comme le principe de la hiérarchisation des risques. Sur 100 risques, on aimerait bien savoir quels sont les dix premiers ? Parce qu'à un moment donné, on ne peut pas s'attarder à tous les risques de façon équivalente (Édouard).

Il établit des priorités. Se baser sur la mission et sur les priorités d'affaires de l'entreprise est une bonne façon de faire la sécurité selon les experts.

Pour les grandes organisations, les priorités ne se limitent pas toujours à certains actifs sur un site. Valérie a dû catégoriser ses sites en termes de risques organisationnels et prioriser d'auditer les sites ayant une criticalité plus élevée que les autres. Les sites sous sa gestion n'ont pas tous la même importance. Ne pouvant pas tous les inspecter rapidement, elle a commencé par ceux qui représentaient les risques les plus importants pour son entreprise. Pour ce faire, elle a tenu compte de certaines caractéristiques de ses sites : le nombre d'employés, les types d'opérations, les pays où ils sont situés, l'historique des incidents, le montant des pertes potentielles, etc.

4.7.6 Visite sommaire des lieux

Étant sur les lieux, l'expert en profite pour faire une visite sommaire. Idéalement, il est accompagné par un employé qui a une bonne connaissance de l'organisation et qui est en mesure de répondre à ses questions. Cette visite a pour but de familiariser l'expert avec le site pour qu'il ait une meilleure idée de la tâche qu'il aura à accomplir.

4.8 Guide de sécurité (liste de contrôle)

Tous les experts que nous avons rencontrés utilisent un guide de sécurité (liste de contrôle) lorsqu'ils auditent une organisation. Les anglophones utilisent le terme

'check-list' pour nommer cet outil. Le guide de sécurité est une liste de questions au sujet de la sécurité d'une organisation. Il prend différentes formes selon l'expert qui le prépare ou les mandats octroyés. Certains sont généraux et couvrent différents éléments. D'autres sont plus spécifiques et cherchent à approfondir des éléments particuliers. Sébastien a eu à développer un guide spécifique pour inspecter toutes les portes de l'un de ses sites. Il s'est aidé des standards développés par la GRC pour construire sa grille de questions. Édouard utilise des guides spécifiques lorsqu'il effectue un mandat qui se limite à des points bien précis à investiguer. Par exemple, s'il inspecte une entreprise pour vérifier si elle se conforme aux normes C-TPAT, il construit son guide en fonction de ces normes. Valérie a des programmes plus spécifiques pour protéger les informations ayant une grande valeur ou pour protéger les employés ayant à voyager dans des zones à risques.

4.8.1 Guide adapté à l'organisation

Pour développer leurs listes de contrôle, plusieurs experts ont utilisé les listes disponibles via la littérature spécialisée ou par l'intermédiaire d'Internet. Ils s'inspirent des livres et des ressources d'ASIS International. Ils recommandent d'utiliser ces exemples de listes, mais de les adapter à l'organisation auditée. Il est risqué d'utiliser intégralement une liste de contrôle qui n'est pas adaptée à un mandat :

> Même si un guide d'inspection de sécurité peut être un passe-partout dans bien des cas, je pense qu'il doit être élaboré sur mesure pour répondre aux objectifs du projet. Donc, il y a peut-être trois mille questions qui sont potentiellement pertinentes à tous mandats confondus, tous projets confondus. Mais ce n'est pas vrai que tous les projets exigent d'inspecter les mêmes éléments et de poser les mêmes questions dans le cadre de la démarche (Édouard).

Les organisations ont toutes des caractéristiques propres à elles et les guides doivent être conçus en tenant compte de ces différences. Karine utilise des guides qui sont adaptés à chacun de ses sites. James exclut de son guide les questions qui ne sont pas pertinentes pour un mandat. Il explique que ce n'est pas le temps de trier les bonnes questions des mauvaises lorsque nous sommes devant les sujets à rencontrer. Certains

experts utilisent le même guide peu importe le site, mais ne posent pas les questions qui n'ont pas d'intérêt.

4.8.2 Évolution de l'outil

Le guide est un outil qui change au fil du temps. Sylvio le modifie à chaque année et prend en considération tous les changements effectués dans son organisation. Son entreprise évolue si rapidement qu'il est impensable pour lui d'utiliser un outil vieux d'un an. En une année, il a compté plus de 75 changements ayant un impact sur la sécurité. Bien qu'il travaille sur le site, plusieurs changements ont été faits sans qu'il s'en aperçoive. L'expert porte une attention particulière aux changements. Le guide doit évoluer avec l'organisation.

4.8.3 Format du guide

Le format varie d'un guide à l'autre. Celui développé par Valérie est constitué de questions fermées uniquement. Les questions fermées se répondent par 'oui', 'non', 'partiellement' ou 'non applicable'. Sylvio y incorpore des questions ouvertes qui l'amènent à répondre par de courtes phrases. Le nombre de questions varie entre 100 et 300 questions pour un guide général complet. Le guide d'Édouard compte entre 100 et 200 questions selon le mandat. La liste de Sébastien compte 100 questions et celle de Sylvio 300. Valérie utilise le même guide pour tous ses sites pour uniformiser sa collecte de données et il compte 150 questions générales. Elle ne peut pas se permettre de faire des analyses plus pointues :

> Quand tu es en affaires dans le privé, limité par le temps, il faut que tu ailles avec les priorités. Je ne sais pas si tu connais la loi de Pareto ? Mais nous autres on considère qu'avec ce qu'on a comme outils, on est capable de gérer 80 % des besoins et des risques. Il va tout le temps en manquer et on va tout le temps en oublier. Mais des fois on modifie le questionnaire. On ajoute des questions quand on prend connaissance des choses qu'on manque. Mais oui on considère qu'on attrape un bon 80 % (Valérie).

Ayant beaucoup de sites à gérer et ne pouvant souvent pas consacrer plus d'une journée par site pour effectuer l'audit, le guide est circonscrit à l'essentiel. Valérie a beaucoup trop d'actifs à gérer et il lui est impossible de faire une analyse détaillée de chacun. Le guide lui fournit un aperçu des problématiques.

Comme le suggère Geiben et Nasset (1998), Simon, Cynthia et Édouard développent leurs guides de façon à inspecter les organisations de l'extérieur vers l'intérieur. Les questions portent d'abord sur l'environnement extérieur puis vont jusqu'au cœur des opérations.

La majorité des guides utilisés par les experts sont développés sur papier. Seule Valérie a un guide informatique qui est complété à l'ordinateur par ses responsables de la sûreté à travers le monde. Les résultats de l'audit lui sont rapidement transmis. Ne pouvant pas trouver une application qui répondait aux besoins de son entreprise, elle a dû en développer une elle-même. Les applications disponibles sur le marché sont conçues pour faire une analyse détaillée des actifs, ce qui lui était impossible d'effectuer.

4.8.4 L'expert derrière l'outil

Tous les experts s'entendent pour dire que le guide de sécurité est un bon outil. Il s'agit d'un bon aide-mémoire qui facilite la cueillette des données. Toutefois, l'expert qui l'utilise doit avoir un minimum de compétences afin de répondre adéquatement aux questions :

> C'est un excellent, c'est un bon outil, c'est un bon 'reminder', mais ça n'enlève pas la perspicacité du gars en arrière de l'outil (Sylvio).

L'expert doit avoir les connaissances pour utiliser le guide de sécurité de façon optimale (James). Il doit être en mesure de bien analyser l'organisation et de poser les bonnes questions. Les réponses à la même question peuvent varier d'un expert à l'autre. Par exemple, la réponse à la question 'est-ce que l'éclairage est adéquat ?' peut

varier selon la perception que les experts ont de l'éclairage sur le site (Valérie). Une personne ayant une bonne expertise sera davantage en mesure de reconnaître si l'éclairage est adéquat ou s'il y a des lacunes à ce niveau.

4.8.5 Exemple de guide de sécurité

Le guide de sécurité (liste de contrôle) est un outil qui est largement utilisé par les experts lorsqu'ils ont à faire le relevé d'une organisation. Tous les experts qui ont été rencontrés utilisent cet outil qu'ils trouvent très utile, voire indispensable. Pour cette raison, nous jugeons utile d'inclure à ce mémoire un exemple de liste de contrôle générale. Elle est conçue de manière à procéder à l'examen de l'organisation de l'extérieur vers l'intérieur, comme le proposent Geiben et Nasset (1998 : 98).

Exemple de guide de sécurité (liste de contrôle)[3]

Date et lieu :
Nom de l'organisation :
Lieu(x) audité(s) :
Nom de la personne interviewée :
Coordonnées de cette personne :
Durée de la rencontre :

a. Informations générales sur l'organisation
-Quel est le secteur d'activités ?
-Quelles sont les opérations les plus importantes ?
-Quelle est sa mission?
-Quels sont les mandats et l'orientation stratégique ?
-Combien y a-t-il d'employés ?
-Quelle est la superficie du site ?

1. Sources de données, d'informations et de statistiques (sources extérieures et internes)
a)Est-ce qu'il y a des sources extérieures en mesure de fournir des informations ou des statistiques, comme par exemple des données sur la criminalité ?
i) Sources policières
ii) Assurances
iii) Médias
iv) Organisations similaires
b) Est-ce que l'organisation tient l'historique de ses incidents, ou possède tout autre base de données sur ses pertes ?
c) Est-ce qu'il y a des problèmes de sécurité importants ?
d) Est-ce qu'il y a une concentration d'incidents dans le temps ou dans l'espace ?

[3] Guide de sécurité tiré du chapitre 26 du *Traité de sécurité intérieure* (Mignault 2007 : 392-396)

e) Qui sont les délinquants qui affectent ou risquent d'affecter l'organisation ?
   i) Comment opèrent-ils ?
   ii) Combien sont-ils ?
   iii) Est-ce qu'il s'agit d'employés dans l'organisation, de clients, de contracteurs ou de personnes externes ?

f) Quelles sont les cibles actuelles ou éventuelles sur le site ?

2. Milieu environnant

a) Est-ce que le climat peut avoir un impact sur la sécurité de l'entreprise (possibilité de vents violents, de pluie abondante, de brouillard, de sécheresse) ?

b) Est-ce qu'il y a des caractéristiques géographiques qui peuvent avoir un impact sur la sécurité (faille sismique, cours d'eau) ?

c) Quelles sont les caractéristiques sociales ou politiques de la région (tension politique, tension sociale, guerre, taux de criminalité) ?

d) Est-ce qu'il y a des services d'urgence à proximité (police, pompiers, hôpital) ?

e) Le site est-il isolé, situé dans un milieu industriel ou dans un milieu urbain ?

f) Quelles sont les infrastructures avoisinantes (autoroute, voie ferrée, aéroport, aqueduc) ?

g) De quoi est constitué le voisinage (présence d'industries, de commerces, d'habitats, d'écoles, de centres commerciaux) ?

h) Est-ce que le secteur à l'extérieur du périmètre est bien éclairé ?

3. Périmètre de sécurité

a) Le périmètre est-il délimité par une clôture, un mur, une haie dense ?

b) Des contrôles d'accès sont-ils en place ?

c) Des capteurs sont-ils installés pour détecter la présence d'un intrus ?

d) Est-ce qu'il y a un stationnement ? Si oui, est-il contrôlé ?

e) Est-ce qu'il y a des végétaux ou des structures grâce auxquels un intrus pourrait se cacher ?

f) Comment les lieux sont-ils entretenus ?

g) Le périmètre est-il partout éclairé ?

h) Un système d'alarme permet-il de détecter les intrus ?

i) Des gardiens ou des chiens patrouillent-ils le périmètre ?

4. Contrôle d'accès

a) Les employés et les visiteurs sont-ils contrôlés ? Si oui, comment ?

b) Sont-ils fouillés ?

c) Y a-t-il un registre des visiteurs ?

d) Les employés ainsi que les visiteurs sont-ils identifiés à l'aide de cartes ?

e) Y a-t-il un système de contrôle d'accès (carte magnétique, code d'accès) ?

5. Bâtiment

a) Le bâtiment est-il partagé avec d'autres locataires ? Si oui, qui sont-ils ?

b) Les portes et fenêtres facilement accessibles sont-elles sécurisées, renforcées ?

c) Quels types de portes et fenêtres y a-t-il ?

d) Quels types de serrures y a-t-il?

e) Le toit est-il accessible ? Est-il possible d'entrer par le toit ?

f) Les sorties de secours sont-elles conçues pour permettre une évacuation rapide et pour empêcher les personnes non autorisées d'entrer ?

g) Les échelles de secours sont-elles accessibles ?

h) D'autres accès peuvent-ils être empruntés pour accéder à l'intérieur du bâtiment (accès sous terrain, conduite d'aération, air climatisé, système de chauffage, drain, égout) ?

i) Un système d'alarme protège-t-il le bâtiment ?

j) Est-ce qu'il y a des zones sécurisées à l'intérieur du bâtiment ?

6. Éclairage
   a) L'éclairage est-il efficace la nuit ?
   b) L'éclairage laisse-t-il des zones ombragées, sombres, ou trop éclairées (éblouissantes) ?
   c) Les endroits stratégiques sont-ils davantage éclairés ?
   d) Est-ce que les installations sont vérifiées et entretenues ?
   e) Une source d'alimentation est-elle prévue en cas de panne électrique du réseau ?
      i) Permet-elle de maintenir toutes les sources d'éclairage ?
      ii) Combien de temps cette source peut-elle pallier le problème ?
   f) Y a-t-il un éclairage spécial prévu en cas d'urgence ?

7. Système d'alarme
   a) Y a-t-il un système d'alarme ? Quelles zones sont couvertes par ce système ?
   b) Lorsque l'alarme est déclenchée, y a-t-il une sirène ou une lumière qui s'allume pour indiquer l'endroit où l'évènement se produit?
   c) Le système d'alarme est-il relié à une centrale prévue pour gérer les alarmes 24 heures sur 24 ?
   d) Quelle est la procédure de réponse aux alarmes ?

8. Télésurveillance
   a) Est-ce qu'il y a des caméras de surveillance sur le site ?
   b) Combien y a-t-il de caméras et où sont-elles placées ?
   c) Les caméras peuvent-elles pivoter et faire des zooms ?
   d) Est-ce que la qualité des images est suffisante ?
   e) La visibilité des espaces surveillés par les caméras est-elle suffisante ?
   f) Est-ce que les images sont enregistrées ? Si oui :
      i) Combien de temps les images sont-elles conservées ?
      ii) Sur quel support les images sont-elles conservées ?
      iii) Les enregistrements sont-ils en sécurité ?
   g) Est-ce qu'il y a des personnes qui visionnent les images en temps réel ?
   h) Y a-t-il une centrale de surveillance et, si oui, comment opère-t-elle ?
   i) À la vue d'incidents en temps réel, quelle est la politique d'intervention ?
   j) Intervient-on réellement ?
   k) Les espaces sous surveillance réunissent-ils les conditions de visibilité (éclairage, vue dégagée de tout obstacle) ?
   l) Comment le système de télésurveillance est-il coordonné aux autres éléments de la sécurité et au personnel?

9. Autres équipements de sécurité
   a) La biométrie est-elle utilisée ?
   b) Est-ce qu'il y a des portiques pour la détection du métal ?
   c) Le GPS est-il utilisé ?
   d) D'autres équipements sont-ils utilisés (étiquettes électroniques) ?

10. Entreposage des biens et valeurs
   a) Quels sont les biens les plus susceptibles d'être volés ?
   b) Est-ce qu'il y a des caisses enregistreuses pour recevoir l'argent des clients ?
   c) Une procédure est-elle imposée aux caissiers afin qu'ils gardent une somme maximale dans leur tiroir-caisse ?
   d) Y a-t-il un coffre ou une voûte pour conserver les biens de valeur et l'argent ?

e) La marchandise est-elle contrôlée à la réception ?
f) L'entrepôt pour conserver les produits, l'équipement et les outils est-il bien sécurisé ?
g) Des contrôles et des inventaires sont-ils faits régulièrement ?
h) La sortie du matériel est-elle contrôlée ?

11. Informatique (matériel informatique, logiciels et informations)
a) La salle des serveurs informatiques est-elle protégée ?
b) Est-il possible de verrouiller les ordinateurs ?
c) Des programmes de sécurité sont-ils installés sur les ordinateurs et les serveurs ?
d) Les ordinateurs sont-ils dotés de coupe-feu ?

12. Protection des informations
a) Où sont entreposés les documents confidentiels ?
b) Les documents confidentiels sont-ils déchiquetés après leur utilisation ? Si oui, par qui et comment ?

13. Communication
a) Les moyens de communication sont-ils disponibles en tout temps (téléphone, Internet, radio, télévision) ?
b) Y a-t-il des boutons paniques reliés au bureau de la sécurité ou à une centrale externe en cas d'urgence ?

14. Mesures d'urgence
a) Y a-t-il un plan d'évacuation développé et connu des employés ?
b) Les procédures d'urgence sont-elles mises en pratique périodiquement ?

15. Personnel de sécurité
a) Y a-t-il des employés attitrés à la sécurité à temps plein ou à temps partiel ?
b) Les employés sont-ils embauchés par l'organisation ou travaillent-ils à contrat pour une agence externe ?
c) Quel est leur salaire ?
d) Combien d'employés sont affectés à la sécurité ?
e) Les employés ont-ils des outils pour intervenir et se défendre ? Si oui, lesquels ?
f) Les employés sont-ils bien formés ?
g) Quelles sont leurs tâches, quel est leur mandat ?

16. Ressources humaines
a) En quoi consiste le processus de sélection de tous les employés ?
i) Le processus est-il rigoureux ?
ii) Des tests et entrevues sont-ils prévus ?
iii) Une enquête de sécurité est-elle effectuée ?
iv) Y a-t-il une entente de confidentialité et de non-concurrence avec les employés ?
v) Y a-t-il un programme de dépistage des drogues ?
vi) Est-ce que le casier judiciaire de chaque employé est vérifié ?

17. Fournisseurs de services
a) L'entretien ménager est-il exécuté par le personnel d'une entreprise externe ?
b) Le ramassage des ordures se fait-il dans le périmètre de sécurité ?
c) Un service de déchiquetage de documents est-il utilisé ?

Toute organisation devrait être inspectée à l'aide d'un guide conçu sur mesure. Quand vient le temps de développer un guide pour son employeur ou pour un client, il est recommandé de consulter les différents exemples qui se trouvent dans la littérature. Il est impératif de les adapter aux besoins de l'organisation pour aller chercher les bonnes informations et pour éviter les pertes de temps durant la cueillette des données.

4.8.6 Le guide d'inspection et la prévention situationnelle

Les experts en inspectant une organisation à l'aide d'un guide d'inspection exercent une forme de contrôle social et utilisent les concepts de la prévention situationnelle. Plusieurs éléments répertoriés dans les guides de sécurité sont des moyens rattachés à la prévention situationnelle et peuvent être insérés dans les catégories de moyens répertoriées par Cusson (2002) : la surveillance et les vérifications ; les protections physiques ; les contrôles d'accès ; les contrôles de facilitateurs ; les détournements et les désintéressements. Par exemple, l'expert en corrigeant les lacunes rattachées à la télésurveillance rend le crime plus risqué. Par exemple, ayant des caméras fonctionnelles et du personnel qui regardent les moniteurs, une organisation se prévient du crime. En analysant l'organisation, en trouvant les différentes forces et faiblesses au niveau de la sécurité et en recommandant des mesures visant à renforcir la sécurité, ils rendent les crimes plus difficiles ou risqués à commettre ou encore moins payants. Le criminel sera dissuadé et ne poursuivra pas ses activités criminelles contre l'organisation si après avoir effectué son calcul coûts/bénéfices il se rend compte que le jeu n'en vaut pas la chandelle. Si quelques experts sont davantage en mesure de comprendre cet effet dissuasif, les autres en auditant les organisations à l'aide des guides de sécurité appliquent tout de même ces concepts criminologiques même s'ils les maîtrisent moins.

4.9 Terrain

La démarche sur le terrain est essentielle pour rechercher les informations et les données qui permettent à l'expert de se faire une bonne image de l'organisation, de son

fonctionnement, de ses opérations et de son niveau de sécurité. C'est à cette étape qu'il documente les forces et les faiblesses. La cueillette d'informations ne se limite pas au site, mais s'étend aussi à l'environnement dans lequel l'organisation se situe. Cette démarche occupe une partie importante du temps consacré au projet :

> Cinquante pour cent au moins va être sur le terrain. Si vous ne le faites pas. Si vous faites une étude de sécurité et que vous faites 2 % sur le terrain, il manque quelque chose. Quand on parle du terrain, on parle de rencontrer des gens, de visiter les lieux, de voir, de comprendre comment ça fonctionne (James).

L'expert se rend sur les lieux et prend le temps qu'il faut pour recueillir les informations. Il ne peut pas faire cette démarche uniquement à partir de son bureau :

> Parce que ça ne se fait pas à partir des bureaux. Le bureau c'est une dangereuse place pour conduire le monde (Gérald).

James compare cette démarche terrain au travail qui est fait par les arpenteurs. Il est primordial d'aller « marcher le périmètre » ajoute Gérald. Par marcher le périmètre, les experts entendent aller investiguer l'ensemble du terrain.

4.9.1 Informations recherchées

Premièrement, il est conseillé de faire un bon inventaire des menaces inhérentes à l'organisation et à son secteur d'activités:

> Les menaces doivent s'apprécier avant de faire un inventaire des vulnérabilités, justement pour savoir de façon inhérente quels types d'actifs sont davantage susceptibles d'être victimes de la menace qui peut se concrétiser. Trop souvent, dans le processus d'inspection, on n'a pas fait ce premier tri. De sorte qu'on prend des routes qui peuvent être inutiles en bout de ligne parce que la menace inhérente est trop faible pour qu'on se préoccupe de ces aspects (Édouard).

En identifiant les actifs menacés, l'expert porte une attention plus particulière. Les menaces sont découvertes en analysant les incidents passés de l'organisation, mais aussi en consultant différentes ressources extérieures à l'organisation (Peter).

Pour identifier les crimes susceptibles d'affecter l'organisation, la majorité des experts rencontrés vont chercher les statistiques policières du quartier où est situé le site. Ces statistiques sont analysées de façon à comprendre la criminalité du quartier. Il faut décortiquer ces données et cibler les crimes susceptibles d'affecter l'organisation. James porte attention à la criminalité générale, mais regarde aussi certains crimes plus spécifiques (exemples : crimes contre la propriété et crimes violents). Il est conscient que la criminalité peut diminuer de façon générale, mais que certains crimes peuvent faire l'objet d'une augmentation. Les organisations similaires ou voisines peuvent aussi être consultées. Sylvio et les gestionnaires de sécurité des entreprises similaires à la sienne ont formé un consortium dans le but d'échanger au sujet de la sécurité. Ils se rencontrent pour analyser les problématiques qu'ils partagent en cette matière. Par ailleurs, Peter récolte des informations auprès des gestionnaires en sécurité qui travaillent pour les organisations avoisinantes au site à l'étude.

Dans sa cueillette d'informations, l'expert évalue si les actifs sont vulnérables. À cette étape, certains experts tiennent compte des contre-mesures qui sont mises en place pour protéger les actifs alors que d'autres préfèrent ne pas les prendre en considération pour évaluer les vulnérabilités (Édouard).

4.9.2 Types de données recueillies

Les données recueillies se divisent en deux grandes familles. Il y a les données quantitatives, avec lesquelles il est possible de faire des statistiques, et les données qualitatives :

> Mais souvent les gens ne les complètent pas (rapport d'incidents, statistiques). Parce qu'ils n'ont pas développé de système qui leur permet de les compiler intelligemment pour capitaliser sur l'information

> qu'ils peuvent en tirer pour orienter par la suite les mesures de sécurité (Édouard).

> Je vais aller à l'extrême. Les assureurs vont être à peu près les seuls à pouvoir faire l'évaluation des risques d'une manière quantitative, donc sur la base de faits qui vont conduire à une évaluation des impacts sous une forme monétaire par exemple. Ça c'est le meilleur des scénarios et il ne survient à peu près jamais dans les organisations. Sauf au niveau des assurances. Donc, plus souvent qu'autrement, on est pris pour fonder notre inspection et ultimement l'évaluation des risques sur une approche subjective et qualitative (Édouard).

Beaucoup d'audits sont réalisés sans qu'il y ait eu de données statistiques utilisées. Certains experts aimeraient bien utiliser ces données pour évaluer et analyser la sécurité des organisations. Malheureusement, elles ne sont pas toujours existantes ou suffisamment bien organisées pour pouvoir en tirer des analyses intéressantes (Walsh et Healy 1994 : 2-I-8; ASIS International 2003 : 10-11). Les organisations devraient les colliger de façon à ce qu'elles puissent être collectées et analysées par les auditeurs. Elles permettraient d'obtenir une meilleure connaissance des problématiques, d'effectuer de meilleures analyses des problèmes et éventuellement de faire une évaluation plus juste des résultats. Même s'il est parfois impossible de faire une analyse statistique pour appuyer les recommandations, il faut au moins baser le rapport sur une inspection et une évaluation qualitative (Édouard). Cette façon de faire l'audit est aussi recommandée par ASIS International (2003). Tout comme Édouard, ASIS International suggère de se tourner vers une approche qualitative pour aller chercher les informations.

4.9.3 Méthode qualitative

Quatre techniques de cueillette des données sont utilisées par les experts. Les deux principales sont l'observation et les entretiens avec les employés. La troisième est l'analyse de documents. La sécurité peut aussi être testée.

Rencontre avec les employés

Des employés sont rencontrés durant l'audit. Il ne s'agit pas uniquement de rencontrer le demandeur et les gestionnaires. Il faut aller voir des personnes à différents niveaux dans l'organisation. Ils ont chacun leur manière de percevoir et de vivre les problématiques. L'expert est limité et il ne peut pas rencontrer tous les employés. Idéalement, il choisit une personne par secteur.

Les employés sont en mesure de fournir des informations intéressantes concernant l'organisation qui ne pourraient pas être obtenues par l'observation uniquement. Ils ont une bonne connaissance de leur milieu de travail et de leur expertise (Dimitri, Gérald). Ils peuvent dresser le portrait des incidents passés là où il n'y a pas de rapport d'incident, ni de statistique (Édouard). C'est avec eux que l'expert réussit à répondre au guide de sécurité. Finalement, il faut profiter de ces rencontres pour évaluer si les employés sont ouverts ou non aux éventuelles mesures qui peuvent être mises en place suite à l'audit (Cynthia).

Idéalement, les employés ont connaissance de la venue de l'expert et sont informés de son mandat. L'approche adoptée par le professionnel est très importante lors des rencontres avec les employés. Il doit être en mesure de bien expliquer son travail et de présenter le projet de façon à ce que les employés soient réceptifs et participatifs par la suite (Simon). Les questions sont posées de manière à obtenir le maximum d'informations :

> Tu ne peux pas demander : 'Quand est-ce que vous vous êtes fait voler de l'information cette année ?' 'Ah! je ne le sais pas' Si la personne ne le sait pas. Tu vas dire : À quels endroits dans votre entreprise quelqu'un qui voudrait voler votre information pourrait le faire? (James)

Il faut faire attention à la façon de poser les questions. Il ne faut pas se buter aux premières réponses négatives données par les employés, mais bien continuer à discuter avec eux jusqu'à ce que les informations ressortent. Cynthia et Gérald ont remarqué

qu'au début les gens peuvent penser qu'ils ne sont pas en mesure d'aider alors qu'ils détiennent plusieurs renseignements forts utiles.

Une enregistreuse est parfois utilisée pour conserver le maximum d'informations qui ressortent des entretiens. Toutefois, son utilisation n'est pas toujours conseillée puisqu'elle peut faire en sorte que des employés donnent moins d'informations (Cynthia). Cela est souvent expliqué par la gêne d'être enregistré ou le désir de ne pas transmettre de l'information qui est conservée intégralement par un expert.

Observation

Les séances d'observation consistent à faire la tournée des lieux pour recueillir des informations. L'observation se fait à différents moments et idéalement chaque plage horaire est couverte par l'expert (Peter). Cet exercice est fait le jour, le soir, durant les pauses des employés, sur l'heure du dîner, la nuit, les journées de semaine et aussi les fins de semaine. L'expert peut être accompagné pour obtenir des explications supplémentaires, mais peut aussi faire l'exercice seul (Peter).

L'observation est un excellent moyen de connaître l'organisation et son fonctionnement. Elle est encouragée pour valider ce qui a été dit par les employés durant les rencontres (James). Il peut y avoir un écart entre le discours des employés et la réalité sur le terrain. Les employés peuvent mentir en cachant certaines problématiques ou en embellissant l'état de la sécurité dans leur organisation. À d'autres moments, l'écart est expliqué par une méconnaissance des employés face à la sécurité. En observant, l'expert est en mesure de trouver différentes failles qui sont par la suite exposées dans son rapport.

Les équipements de sécurité sont inspectés. Il s'agit ici de valider la présence des équipements, mais aussi d'en vérifier l'entretien (Valérie). L'expert se questionne sur ce qui pourrait nuire au bon fonctionnement des dispositifs de sécurité en place (Karine). Par exemple, il est plus facile de traverser une clôture si l'organisation

entrepose sa neige à proximité. Par ailleurs, l'expert vérifie si l'équipement est fonctionnel.

Le professionnel porte une attention aux différentes activités qui se déroulent sur le site. Il regarde comment le travail se fait au quotidien, observe la circulation sur le site, vérifie l'utilisation que font les employés des systèmes de sécurité, etc.

Analyse documentaire

Différents documents sont consultés par l'expert (Édouard). La majorité des professionnels consultent les plans de l'organisation durant l'audit. Les procédures ayant un impact sur la sécurité sont lues et comprises (Simon). Les mesures d'urgence sont consultées. Les rapports d'incidents et les inventaires sont d'autres documents intéressants (Sébastien).

Tests de la sécurité

Quoiqu'ils soient plus rares et compliqués, des tests peuvent être effectués pour mettre à l'épreuve la sécurité de l'organisation. Les experts testent alors le bon fonctionnement des équipements ou tentent de percer la sécurité de l'organisation. Ces exercices peuvent être faits par l'expert ou par d'autres personnes. Ils sont toujours approuvés par la gestion.

Outils de travail

Tous les experts, à l'exception de Carol, utilisent un appareil photo numérique pour prendre plusieurs clichés des lieux. Il s'agit d'un outil indispensable que Sylvio complète avec des enregistrements vidéo commentés. Les photos sont utiles pour l'expert, car il peut observer les lieux sans avoir à y retourner (Peter). Il est primordial d'être rigoureux lors de la séance de photos et de les accompagner d'une bonne prise de notes. Il est facile de s'y perdre, de ne plus comprendre pourquoi certaines photos

ont été prises et de ne pas se remémorer où elles ont été prises (Dimitri, Cynthia). En inscrivant le numéro de la photo sur le plan et en l'appuyant par des notes, il est plus facile de s'y retrouver. Les photos insérées dans le rapport sont utiles pour le demandeur qui s'en sert pour mieux comprendre les recommandations. Il est déconseillé d'insérer trop de photographies dans le rapport selon Peter.

Un autre outil très apprécié est le plan de l'organisation. Les experts l'utilisent abondamment lorsqu'ils observent les lieux pour faciliter les déplacements et pour repérer les éléments structuraux (fenêtres, portes, issues de secours, escaliers). Ils y prennent beaucoup de notes (numéros des photographies, numéros pour se référer au calepin de notes, emplacements des équipements de sécurité, location des éventuelles recommandations). Le plan annoté est une excellente référence pour le demandeur qui peut situer ses équipements de sécurité et repérer plus facilement les constats ainsi que les recommandations (Cynthia).

4.9.4 Méthode quantitative

Carol a remarqué que les données quantitatives sont disponibles et utilisées surtout dans les grandes entreprises. James mentionne que nous retrouvons ces données principalement dans les organisations où il y a un service de sécurité depuis un certain temps. Carol et Édouard ajoutent que plusieurs petites et moyennes organisations ne prennent pas le temps de documenter les incidents et ne cumulent pas de statistique. Ces données ne sont pas compilées dans les organisations qui ont un volume trop important d'incidents. Édouard a renoncé à utiliser ce genre de données dans ces entreprises puisqu'ils ne prennent pas le temps d'alimenter les banques de données. Pour ces entreprises, il s'agit d'une perte de temps inutile (Édouard).

Il est important que le système conçu pour recueillir les incidents et les statistiques soit simple et convivial pour les gens qui ont à s'en servir. S'il est compliqué et que les rapports sont trop longs à remplir, les gens ne se donnent pas la peine de rapporter tous les incidents. Sylvio a implanté un logiciel simple à utiliser pour compiler les incidents

et il lui permet d'obtenir des statistiques facilement. Il est simple de travailler avec des données numérisées, ces dernières étant plus faciles à organiser. Kevin partage cet avis et ajoute que l'intérêt de recueillir les données sur papier disparaît.

Les organisations peuvent développer par elles-mêmes des applications informatiques qui vont structurer et archiver les données intelligemment. Valérie avec l'aide d'un informaticien se sont chargés de développer cette application dans leur entreprise. Il est aussi possible d'acheter des logiciels vendus par des entreprises qui développent des applications informatiques conçues pour aider les gestionnaires à gérer la sécurité. Quoique déjà polyvalents, ces logiciels peuvent être modifiés et adaptés à la demande des clients. L'entreprise de Kevin développe de tels logiciels. Ils ont plusieurs utilités. Par exemple, ils permettent d'avoir une idée précise des tâches routinières effectuées par le personnel de sécurité. Il est facile de suivre les rondes effectuées par les agents et d'avoir un meilleur contrôle sur l'utilisation des effectifs. Cela permet de mieux orienter les ressources. Il est aussi possible de compléter des rapports rapidement et d'y attacher des enregistrements vidéo, des rapports numérisés ou des photographies. Ces rapports peuvent être consultés quotidiennement par toutes les personnes qui y ont accès, dont les auditeurs. Ils sont en mesure de vérifier les incidents et de les catégoriser. En faisant une sélection, l'auditeur peut faire ressortir les incidents en fonction de différentes caractéristiques (exemples : les classer selon leur niveau de gravité, de les situer dans l'espace et dans le temps). Les possibilités sont infinies dans ce domaine. S'il est trop compliqué ou coûteux pour plusieurs organisations de développer leurs propres logiciels de sécurité, il est toujours possible pour elles de compter sur les applications informatiques disponibles sur le marché qui facilitent la collecte des données quantitatives et leur analyse. Ces applications sont de plus en plus accessibles pour l'ensemble des organisations. Kevin admet qu'elles sont d'une grande utilité et qu'il s'agit d'outils puissants à considérer lors de la réalisation des audits de sécurité.

La majorité des experts s'entendent pour dire que recueillir et analyser les données quantitatives est une excellente façon de travailler. Cela permet d'avoir une idée plus

précise des problèmes et de la sécurité d'une organisation. Sylvio et Sébastien préfèrent appuyer les constats et les recommandations sur des données lorsqu'ils se présentent devant le demandeur. Cela a plus d'impact auprès des décideurs. En outre, il est plus facile d'évaluer les résultats donnés par les mesures implantées à l'aide des données statistiques.

4.9.5 Importance de la démarche sur le terrain et de la collecte des données

Tout le travail effectué sur le terrain pour collecter les données et les informations sur l'organisation est une étape très importante. Certains professionnels en sécurité n'effectuent pas cette recherche et ne font pas d'analyse rigoureuse :

> C'est sûr qu'en tant que consultant, on se voit mal arriver puis fournir des recommandations sans appuyer les recommandations sur une bonne analyse de la situation. Pourtant, il y a bien des gens qui fournissent un rapport de recommandations et qui n'ont aucune démarche d'inspection et d'évaluation à l'appui. C'est un peu comme s'ils tiraient cela de leur chapeau. Donc, je dirais que ça c'est très subjectif comme approche (Édouard).

Il est préférable de baser les recommandations sur des faits vérifiables, sur une bonne connaissance de l'organisation et sur des standards. S'il est impossible de recueillir des statistiques, il faut au minimum faire une bonne recherche de données qualitatives.

4.10 Analyse des données

Après avoir recueilli plusieurs données, l'expert se questionne avant de poser son diagnostic. Pour améliorer sa compréhension, il analyse et applique des concepts qui vont l'aider à mieux interpréter les informations.

4.10.1 Application de concepts criminologiques

James documente les incidents pour mieux comprendre et analyser les problématiques. Une fois qu'il a recueilli le maximum d'informations possible au sujet des incidents, il

se questionne à savoir pourquoi ils sont survenus. « C'est toujours le qui, quand, quoi, où, comment et pourquoi qui reviennent » (James). Il utilise les six questions qui sont proposées par Clarke et Eck pour analyser la criminalité (Clarke et Eck, 2003 : chapitre 31).

Pour déterminer si une organisation est à risque ou non, l'expert évalue le milieu dans lequel se trouve le site. Y a-t-il des installations à proximité susceptibles d'attirer des infracteurs (exemples : parc, centre commercial, école secondaire) ? Dans l'éventualité où un délit est commis sur le site de l'organisation, est-ce qu'il est facile pour le délinquant de fuir les lieux (accès rapide au transport en commun, autoroute, artères achalandées) ? Est-ce que le site est isolé ? Les questions à se poser ne se limitent pas seulement à l'environnement, mais s'étendent aux actifs susceptibles d'être affectés (Édouard, James). Quelle est la valeur de l'actif ? Est-il attrayant ou en demande ? L'objet est-il facile à subtiliser (poids, grandeur) ? Plusieurs caractéristiques rattachées à l'environnement et aux actifs peuvent affecter le niveau de vulnérabilité de ces derniers. Les questions qui ont été posées sont susceptibles d'être considérées par les délinquants avant de s'attaquer à une cible. Pour cette raison, il est intéressant de faire cet exercice.

4.10.2 Audit de sécurité et l'analyse des problèmes en criminologie

L'une des différences entre l'analyse des problèmes qui est faite en criminologie et l'audit tel qu'il est réalisé par les experts en sécurité est le point de départ du projet. L'expert en sécurité définie souvent son projet de sécurité à partir d'un lieu, d'un site ou d'une organisation. Il part avec sa liste de contrôle et inspecte les lieux. Les criminologues quant à eux définissent le projet en identifiant les problèmes criminels. Dans le but de réduire le risque que des crimes ne soient commis dans l'avenir, il est possible de mettre en place un programme de prévention en huit étapes (Cusson et coll. 1994 : chapitre 2). Analysons les huit étapes proposées par Cusson et coll. (1994).

La première étape consiste à identifier le problème. Pour Cusson et coll. (1994), un problème criminel est « une activité délinquante spécifique et localisée qui frappe une catégorie de biens ou de personnes et dont l'intensité est telle qu'elle suscite une demande de solution ». Il y aura toujours des crimes qui seront commis dans la société. Ils ne constitueront pas un problème s'ils ne compromettent pas trop la qualité de vie sociale. Là où les criminologues établissent des priorités d'agir, c'est là où la quantité et la gravité des délits affectent de façon plus importante la qualité de vie des citoyens et des organisations. Lorsque nous faisons face à un nombre anormal de plaintes dans un secteur donné, quand un type de crimes survient trop souvent ou quand une organisation subit des pertes trop importantes, il est suggéré de s'arrêter et de vérifier si nous sommes en présence d'un problème criminel. Le fait d'être victimisé une fois dans l'année ne constituera pas en soi un problème. Lorsque nous sommes en face d'une situation problématique intolérable, il faut analyser cette situation afin de trouver les meilleurs correctifs.

La deuxième étape consiste à connaître la nature des délits. Les délits sont commis dans quelles circonstances ? Il s'agit d'analyser les modus operandi des délinquants et de comprendre pourquoi ils s'adonnent à leurs activités.

Troisièmement, le degré de risque est évalué. Si nous ne prenons pas d'action, combien y aura-t-il de délits reliés à notre problématique dans un avenir rapproché ? En vérifiant l'historique des incidents passés, nous obtenons une mesure qui permet d'estimer la probabilité d'occurrence future.

Quatrièmement, le criminologue s'informe au sujet des auteurs des délits. Qui sont-ils ? Que font-ils dans la vie et quelles sont les activités qu'ils pratiquent ? Quelles sont les raisons qui les amènent à agir ainsi ? Ces informations aideront à la recherche de solutions adaptées au problème donné. À l'inverse, et il s'agit de la cinquième étape, il faut identifier les victimes et les cibles. Le criminologue tentera de déterminer les caractéristiques qui font qu'elles sont victimisées plus fréquemment.

Sixièmement, une analyse spatio-temporelle est réalisée. Est-ce qu'il y a des moments ou des endroits où il y a une concentration d'évènements ? En interrogeant les personnes sur le terrain, il est possible d'identifier ces endroits ou ces moments. Il y a aussi des logiciels comme 'mapinfo' qui servent à l'identification des points chauds et facilitent l'analyse spatio-temporelle des problèmes.

Septièmement, une analyse causale du problème est effectuée. Plusieurs causes favorables aux délinquants vont faire en sorte qu'ils vont réussir leurs coups. Il y a des causes lointaines sur lesquelles il est quasiment impossible d'agir et des causes plus rapprochées sur lesquelles nous pouvons plus facilement prendre des actions (Cusson et coll. 1994 : 27).

La dernière étape consiste à faire l'analyse des contrôles sociaux existants. Cette analyse permet d'étudier les mesures préventives et répressives déjà en place dans le but de trouver les forces et les faiblesses des contrôles déjà existants et d'apporter les correctifs nécessaires.

Ce programme en huit étapes a comme objectif d'identifier les problèmes réels, de prendre des actions pour résoudre les problèmes et de protéger les cibles potentielles. Suite à cette analyse, il est plus facile pour le professionnel d'identifier les actions qui permettront d'avoir un réel impact sur les problèmes.

4.10.3 L'approche pragmatique des experts en sécurité privée[4]

Il existe, dans le champ de la sécurité privée, des ouvrages qui traitent des méthodes d'analyse et de la planification des mesures visant à protéger les organisations. Plusieurs experts de la sécurité privée ont écrit à ce sujet. Nous pensons à J. F. Broder, à L. F. Fennely, à M. Garcia, à C. Sennewald ou à C. A. Roper. En criminologie, c'est dans les travaux écrits par des criminologues intéressés à la prévention ou à la

[4] Nous avons utilisé le document 'L'inspection de sécurité et l'analyse d'un problème' rédigé par Maurice Cusson (2005) pour cette partie.

résolution des problèmes que sont traitées les questions d'analyse de risques. Les ouvrages écrits par R. V. Clarke, J. E. Eck, N. Tilley ou M. Cusson sont d'une aide importante quand vient le temps de faire un relevé de sécurité. En combinant ces sources, il est possible d'importer en criminologie l'expertise très pragmatique qui existe en sécurité privée. Réciproquement nous pouvons introduire dans le champ de la sécurité l'expertise en analyse développée en criminologie.

Un travers en criminologie consiste à mener des analyses très élaborées, mais qui ne débouchent pas sur des solutions pratiques. Ainsi voyons-nous le chercheur décrire les tendances, mener des analyses statistiques complexes, mettre la criminalité en rapport avec des variables sociales, démographiques, économiques, etc. Malheureusement, ces analyses ne débouchent pas toujours sur des préconisations réalistes. Dans la mesure où les intervenants n'ont pas de prise sur les variables socio-économiques et démographiques, les analyses des causes lointaines, comme la pauvreté, ne sont pas très utiles pour éclairer l'action (Leman-Langlois 2007 : 368). Le propriétaire d'un petit commerce ne sera pas plus avancé s'il apprend que le problème de vols qui sévit dans son quartier est essentiellement dû à la pauvreté des gens qui habitent les alentours. Ce commerçant n'ayant pas d'impact sur cette variable ne pourra pas régler son problème de vols, à moins qu'il envisage de déménager son commerce. Ce travers s'observe chez les praticiens en sécurité : ils décident d'acheter des équipements ou de recruter du personnel sans analyse préalable et sans identification des problèmes. Pour échapper à de tels pièges, les analyses devraient être menées en gardant à l'esprit des hypothèses de solutions praticables à court et à moyen terme.

L'expert qui réalise un audit de sécurité devrait effectuer des analyses à l'aide des techniques développées par les experts de la sécurité privée et les criminologues. Aucune recommandation ne devrait être faite à un client sans qu'il y ait eu au préalable un minimum d'analyse.

4.10.4 Analyse des risques

L'analyse qui est souvent associée à l'audit de sécurité est l'analyse des risques. Plusieurs experts rencontrés utilisent la façon de faire proposée par ASIS International pour réaliser leur analyse des risques (ASIS International, 2003 : 5). Selon Pierre et James, ce type d'analyse consiste essentiellement à déterminer ce qui doit être protégé, à identifier les menaces, à évaluer la probabilité que les évènements surviennent et l'impact qu'ils peuvent avoir sur l'organisation. Chacun a développé sa propre méthode pour réaliser l'analyse des risques. Dans l'ensemble, la démarche se rapproche des six étapes que nous avons exposées dans la recension des écrits. Les experts classifient les risques selon leur importance et décident lesquels seront pris en charge.

Pour évaluer les probabilités qu'un évènement survienne ou pour en mesurer l'impact, l'expert utilise les données qualitatives et quantitatives collectées sur le terrain. À l'aide de l'historique des incidents, il est plus facile d'évaluer la probabilité qu'un évènement survienne. Dans l'éventualité où l'expert n'a pas de donnée quantitative, il tente d'évaluer les probabilités à l'aide de toutes les informations qui ont été recueillies sur le terrain. Le même travail est fait pour mesurer l'impact. Simon et ses collègues attribuent tous un niveau de probabilité à chacun des risques et en évaluent l'impact. Par la suite, ils comparent leur travail entre eux pour déterminer quels sont les risques qui sont les plus probables et qui ont le plus d'impact sur l'organisation.

4.10.5 Analyse coût/bénéfice

L'analyse coût/bénéfice est importante lorsque vient le temps de choisir les contre-mesures qui seront mises en place. Quelques professionnels font cette analyse. Les avantages liés à l'implantation d'une contre-mesure doivent être supérieurs aux désavantages qui s'y rattachent. Idéalement, Sébastien cherche à rentabiliser les investissements qui sont faits. L'impact de la contre-mesure sur l'organisation est aussi évalué.

4.10.6 Niveau d'analyse

Le niveau d'analyse varie en fonction du mandat. Même si certains experts sont en mesure d'effectuer des analyses plus poussées, ils ne peuvent pas toujours le faire si ce n'est pas dans le mandat. Faire une analyse rigoureuse sur papier exige plus d'investissements. Sans délaisser cette étape importante, l'analyse est souvent faite dans la tête de l'expert tout au long de la cueillette des données. Le demandeur n'a alors pas accès à celle-ci ni au raisonnement qui a été fait par l'expert avant d'arriver aux solutions. Lorsque c'est prévu, l'analyse est explicitée dans un document ou dans le rapport. Cela permet au demandeur de mieux comprendre la méthode d'analyse utilisée par l'expert.

4.11 Rapport

La rédaction du rapport est une étape importante. C'est à l'aide de ce document que le demandeur prend connaissance du travail qui a été fait, du niveau de sécurité de son entreprise et finalement des mesures à prendre pour rendre son organisation plus sécuritaire. Il reflète le bon ou le mauvais travail. Il ne faut pas oublier que ce document porte les noms des experts. Ils se doivent donc de remettre des rapports de qualité. James n'hésite pas à retourner sur le terrain pour vérifier des points qui lui semblent incertains.

Nous avons constaté que deux formes très différentes peuvent être utilisées pour construire le rapport. Le premier type de rapport comporte une dizaine de pages et est très concis. Sébastien et Sylvio rédigent ce genre de rapport. Ils utilisent ce type de rapport puisqu'ils ne peuvent pas se permettre de présenter un rapport plus volumineux. Cette réalité est expliquée par le manque de temps et d'intérêt de la part de la direction des entreprises selon Sébastien. Ce style est principalement utilisé par les experts qui travaillent au sein d'une organisation. Ces derniers se permettent de remettre des rapports plus brefs puisqu'ils travaillent sur place et sont disponibles pour

répondre aux questions par la suite. Un dossier plus volumineux accompagne souvent le projet et il est toujours possible de s'y référer pour éclaircir des points par la suite.

Le deuxième type de rapport est beaucoup plus volumineux (entre 50 et 100 pages). La plupart du temps, les consultants externes rédigent des rapports de ce type (Édouard, James, Simon). Il est davantage considéré comme un produit offert au demandeur et nous y retrouvons beaucoup plus d'informations. Il est souvent accompagné d'un sommaire pour exposer les faits saillants. Plusieurs gestionnaires rencontrés par Simon ne se donnent pas la peine de consulter l'ensemble du rapport et lisent bien souvent les grandes lignes. Dans ce contexte, les résumés sont appréciés.

4.11.1 Le rapport : effort pour les experts

Pour plusieurs experts, la rédaction du rapport est une étape plus difficile à réaliser (Broder 2000). Pour eux il est beaucoup plus facile d'aller chercher les informations que de les communiquer. Il n'est pas toujours évident de structurer toutes les informations et de rédiger un rapport cohérent. Peter a remarqué que la charge de travail peut paraître insurmontable. Pour ne pas se décourager, il recommande de commencer le rapport le plus rapidement possible et de ne pas attendre à la fin de la cueillette des données pour le débuter. Pour d'autres, c'est davantage au niveau de l'écriture que ça accroche. James avoue avoir de la difficulté lorsque vient le temps de communiquer les résultats de son travail à l'écrit.

4.11.2 Informations qui s'y trouvent

Idéalement, le rapport n'est pas constitué uniquement de recommandations. Le contexte qui explique pourquoi un audit est effectué est expliqué. Qui demande l'audit et pourquoi ? Le but est aussi exposé. Le mandat est défini et les gens doivent comprendre ce qui a été inclus et exclu du mandat. Ainsi, ils savent à quoi s'attendre dès le départ. Par la suite, la méthodologie utilisée par l'expert est expliquée. Comment les données ont-elles été amassées ? Finalement, nous retrouvons les

constats et les recommandations. Une façon intéressante de les présenter a été suggérée par Cynthia, Myriam et James. Ils procèdent en trois étapes. Premièrement, ils apportent un constat. Deuxièmement, ils expliquent pourquoi il s'agit d'une problématique pour l'organisation. Pour terminer, ils recommandent des mesures pour régler le problème. Il est important pour eux que le client comprenne le raisonnement derrière chaque recommandation. Ils utilisent aussi des recherches et des statistiques pour appuyer les constats et les recommandations. Par exemple, l'étude de Grandmaison et Tremblay (1997) peut être citée pour justifier le bon ou le mauvais usage de la télésurveillance sur un site.

4.11.3 Présentation du rapport

Nous avons remarqué que le rapport comporte différentes sections : lettre de présentation, introduction, méthodologie, constats, recommandations et conclusion. Des annexes peuvent être jointes pour ne pas alourdir inutilement le texte. Cynthia joint à ses rapports un lexique pour définir les mots techniques qu'elle emploie. Elle annexe aussi des plans du site annotés dans le but de mieux faire comprendre les constats et les recommandations. Si c'est pertinent, Simon incorpore en annexe les photos qu'il n'a pas intégrées dans le rapport.

Les experts portent une attention particulière à la qualité de la présentation et à l'impression du document. Les gens n'aiment pas lire des brouillons. Une belle présentation aide à vendre les recommandations.

Le dépôt du rapport est presque toujours accompagné d'une courte présentation pour le demandeur et les décideurs concernés. Une rencontre est prévue à la fin pour que le demandeur puisse prendre connaissance du rapport et poser ses questions.

4.11.4 Qualité du rapport

Comme Broder (2000, chapitre 8), James aime les rapports qui sont concis, clairs, précis et faciles à lire. Il porte une attention au ton utilisé. Il tente d'être diplomate lorsqu'il fait ses constats et ses recommandations. Selon lui, les employés des organisations n'aiment pas lire des documents accusateurs. Une attention est aussi portée aux mots qui sont employés pour décrire les constats. L'audit n'est pas un exercice ayant pour but de décourager le demandeur. Les mots employés doivent décrire le mieux possible la réalité perçue sur le terrain. Des mots comme 'grave', 'problème', 'critique' ou 'fatal' sont à utiliser avec prudence.

4.12 Recommandations

Une panoplie grandissante de solutions est disponible pour sécuriser une organisation. Une fois que les éléments à sécuriser et que les problèmes ont été identifiés, l'expert propose des mesures qui peuvent être simples, mais aussi très complexes. James et Carol tiennent compte de leur expérience et de plusieurs facteurs avant de faire les recommandations. Idéalement, les problèmes ne sont pas exposés sans être accompagnés de contre-mesures. Les gestionnaires n'aiment pas recevoir des constats négatifs s'il n'y a pas de solution pour corriger la situation.

4.12.1 Types de solutions

Pour sécuriser une organisation selon Carol, il est essentiel d'avoir des personnes, des systèmes et des procédures. La sécurité repose non seulement sur les personnes qui en sont responsables, mais bien sur tous les employés de l'organisation. Les gens sont informés et sensibilisés aux enjeux reliés à la sécurité. Ils doivent être conscients qu'ils ont un impact important sur le niveau de sécurité de leur organisation. Cet impact peut être positif ou négatif. Les systèmes englobent tous les éléments qui améliorent la sécurité, de la simple clôture aux systèmes technologiques. Il arrive que des systèmes de sécurité soient déjà en place dans l'entreprise, mais qu'ils soient mal utilisés. Il

s'agit alors de les repositionner ou de les réactiver. Finalement, des procédures sont en place pour que les employés s'y conforment.

4.12.2 Mesures innovatrices

Les mesures de sécurité dites innovatrices se démarquent de celles plus conventionnelles par leur originalité. De plus, elles nécessitent souvent moins d'investissement. Les experts que nous avons rencontrés aiment donner des exemples de mesures innovatrices qu'ils ont implantées dans le passé, surtout si elles se sont avérées efficaces. Nous croyons qu'ils agissent ainsi pour démontrer leur originalité et leur compétence, mais aussi pour nous convaincre qu'ils ne sont pas là pour recommander des mesures qui sont toujours coûteuses. Nous avons entendu à quelques reprises l'exemple cité par Shearing (2000 : 204-205). Il s'agit du cas où un directeur de la sécurité d'une entreprise a opté pour une mesure qui sortait de l'ordinaire pour régler un problème de vols d'outils. Ces vols étaient perpétrés par les employés de la compagnie. Il avait été découvert qu'ils subtilisaient l'équipement pour effectuer leurs rénovations. Installer des systèmes pour identifier les infracteurs dans le but de les poursuivre devant la justice ne fut pas l'option choisie par ce directeur. Il opta plutôt pour la création d'une banque d'outils que les employés étaient autorisés à emprunter pour leur usage personnel. Cela régla le problème. Durant la conférence donnée par ASIS International, un conférencier nous a raconté qu'il s'est retrouvé devant une situation où son client lui a demandé d'installer des caméras de surveillance pour surveiller les camions stationnés sur le terrain de l'entreprise. La marchandise dans les remorques avait fait l'objet de vols. Cet expert a plutôt suggéré à son client de positionner ses camions différemment de façon à ce qu'il soit impossible pour les voleurs de s'introduire dans les remorques. Cette procédure élimina le problème. Son client n'a pas eu à investir pour installer le système demandé et ni à se préoccuper de visionner les moniteurs par la suite.

4.12.3 Solutions pour une sécurité parfaite ?

Des recommandations sont faites pour régler les problèmes de sécurité inacceptables pour l'organisation tout en acceptant des risques résiduels. Cynthia insiste sur le fait qu'il est sain d'accepter cette partie du risque qui demeure même après avoir sécurisé un site. Il est impossible et irrationnel de chercher à sécuriser parfaitement l'ensemble des actifs :

> Alors, la sécurité parfaite n'est pas un objectif rationnel. Sécurité parfaite égale fonds infinis et irritants majeurs. Aucun organisme n'a des fonds infinis (Dimitri).

La surprotection amène des dépenses importantes et des irritants que les organisations ne peuvent pas accepter. Un exemple d'irritant donné par Carol et Dimitri est l'installation d'un système biométrique pour contrôler les accès. Premièrement, il s'agit d'un système qui est coûteux. Deuxièmement, les opérations sont ralenties puisque les employés sont davantage contrôlés lors de leurs déplacements. Troisièmement, la gestion de ce système peut nécessiter l'affectation d'un employé à temps plein. Quatrièmement, les employés peuvent s'objecter au fait de fournir des informations personnelles (empreintes digitales, échantillon de voix). Avant de faire des recommandations, il est primordial de se questionner sur l'impact qu'elles peuvent avoir sur l'organisation. Est-ce que c'est vraiment nécessaire ? Si oui, il faut chercher à avoir le minimum d'effets négatifs sur l'organisation et ses opérations.

4.12.4 La rentabilisation de la sécurité

La question monétaire revient toujours lorsqu'il est question de corriger un problème de sécurité. La sécurité est souvent perçue comme étant uniquement une dépense alors que c'est faux. Il est possible de rentabiliser les investissements qui sont faits dans ce domaine. Les experts cherchent à trouver des mesures rentables pour l'entreprise et à démontrer aux décideurs qu'elles le sont. Les recommandations qui nécessitent de gros investissements sont justifiées.

4.12.5 Pouvoir décisionnel

Une fois que les recommandations ont été faites, c'est au demandeur à décider des problèmes qu'il souhaite gérer. Cette gestion est faite par le client dans le cas où c'est un consultant qui a fait l'audit ou par les patrons de l'expert qui travaille dans une organisation. L'expert peut accompagner les décideurs pour les aider à prendre ces décisions. Dans d'autres cas, c'est le professionnel qui prend les décisions. Dans son entreprise, Sylvio décide et détermine ce qui doit être fait suite à l'audit.

Les professionnels cherchent à savoir ce qui est susceptible d'être accepté par le demandeur. Les recommandations sont choisies et présentées de façon à ce que le demandeur s'y intéresse :

> Au niveau des recommandations, moi je dis toujours, lorsqu'on fait une analyse de risques, ce qui est important c'est d'essayer de comprendre la position des gestionnaires de l'entreprise. Il faut tenter de se placer dans la chaise du gestionnaire qui va avoir à prendre une décision pour comprendre exactement qu'est-ce qu'il va influencer ses décisions à lui. Il ne faut pas arriver avec des recommandations qui vont être farfelues. Il n'ira pas de l'avant (Pierre).

Il est suggéré de se mettre à la place du décideur et de se questionner à savoir si nous accepterions les solutions que nous nous apprêtons à recommander. Les demandeurs n'aiment pas recevoir des recommandations impossibles à exécuter.

Sébastien et Cynthia informent le demandeur des implications qu'amènent les recommandations. Quel en est le coût ? Est-ce que ça implique l'embauche d'employés ? Est-ce que les employés sont favorables aux mesures ? Est-ce qu'une formation doit être donnée ? Comment ça fonctionne ? Pourquoi ces recommandations ? Est-ce que c'est légal ? Est-ce que ça respecte la réglementation municipale ? Idéalement, l'expert est le plus transparent possible et soulève tous les points qui aident le demandeur à prendre la meilleure décision possible. Pour sa part, Simon donne le minimum d'informations sur chacune des recommandations jugeant qu'il ne sait pas à cette étape lesquelles seront choisies par le demandeur. Il se limite à donner

des recommandations très générales. Si le client décide d'implanter certaines mesures, il lui fournit plus d'informations dans un autre mandat. L'implantation des mesures est un mandat distinct pour lui et c'est à cette étape qu'il faut expliquer comment mettre les recommandations de l'avant. Édouard est du même avis :

> Ça n'exclut pas que dans la phase 1, au terme de notre évaluation des risques, qu'on fournisse des grandes recommandations. Mais on n'ira pas au point de détailler la quantité, les spécifications de technologie de la sécurité. C'est inutile parce que le client, dans le fond, en fait nous ça serait plus intéressant financièrement parce qu'on charge plus cher parce qu'on passe plus de temps. Sauf que ce ne serait pas logique de le faire tant que le client n'a pas décidé s'il adressait ou non tel ou tel risque (Édouard).

Pour Édouard et Simon, il est inutile de perdre trop de temps à expliquer en détail les mesures recommandées et d'expliquer comment les implanter. À ce stade, il est préférable de simplement en donner un aperçu au demandeur.

4.12.6 Surprise des gestionnaires

Les constats doivent être bien expliqués aux gestionnaires afin d'éviter une incompréhension de leur part. Les constats peuvent en effet être mal interprétés par le demandeur. Par exemple, la direction peut penser qu'elle est en mesure de diminuer ses dépenses au niveau de la sécurité s'il lui est rapporté qu'il n'y a pas de problème de sécurité et que ça va bien à ce niveau (Carol). À l'inverse, la direction peut avoir une impression que le niveau de sécurité a diminué suite à l'instauration d'un service de sécurité au sein de son entreprise (James). Le service de sécurité en sensibilisant davantage les gestionnaires face aux différents problèmes peut leur laisser croire que la situation se dégrade dans l'organisation.

4.12.7 Solutions alternatives

Pour différentes raisons, l'expert peut se voir contraint de ne pas recommander la solution qui lui paraît idéale. Elle peut représenter des coûts qui sont trop importants. Il

peut aussi anticiper qu'elle ne sera pas bien acceptée par les employés et qu'elle sera par conséquent inefficace. Lorsqu'une telle situation survient, Cynthia et Carol proposent une solution optimale et soulèvent les problématiques qui lui sont rattachées tout en amenant des alternatives.

4.12.8 Planification dans le temps

À cause d'un manque de temps ou d'argent, l'implantation de certaines recommandations peut être reportée dans le temps. D'autres raisons expliquent le report des recommandations. Par exemple, Carol tente de ne pas apeurer le client en lui proposant trop de mesures d'un seul coup. James établit un échéancier et le demandeur implante les mesures au fur et à mesure que c'est possible. Pour commencer, il tente de régler les problèmes qui causent les inquiétudes immédiates. S'il y a des éléments à ajouter, il y va graduellement. La sécurité peut être peaufinée sur des années. Si c'est possible, il est préférable d'agir graduellement pour ne pas effrayer les employés (Sébastien). Ces derniers risquent de s'objecter aux changements trop importants qui s'étalent sur une courte période de temps.

4.13 Fin du projet d'audit

Plusieurs experts s'entendent pour dire que l'audit se termine au moment où le rapport est déposé. Tous les mandats et les autres projets qui suivent le dépôt des recommandations ne sont plus considérés comme faisant partie de l'audit initial.

4.14 L'audit et la recherche en criminologie

Plusieurs criminologues se sont penchés sur des questions pouvant intéresser les experts de la sécurité privée qui ont à auditer des organisations. Pensons à un professionnel qui a à inspecter un hôpital dans le but d'évaluer sa sécurité. Il peut lui être profitable de consulter les travaux de Roger Le Doussal qui s'est intéressé à la sécurité des hôpitaux et aux différents problèmes de sécurité que nous y trouvons (Le

Doussal : 1991, 1995a, 1995b; Le Doussal et Laures-Colonna 1992). Plusieurs ouvrages de Maurice Cusson méritent leur place dans la bibliothèque des experts (Cusson : 2002; 2005; 2007, chapitres 27, 28, 29 et 31). Nous y retrouvons plusieurs bonnes façons de faire ayant été évaluées et testées au fil des années. Les travaux des criminologues sont une source d'aide et d'inspiration. Il est encouragé de citer ces spécialistes dans le rapport final. Cela a pour effet de donner davantage de crédibilité aux constats et aux éventuelles recommandations. Les gestionnaires se sentiront réconfortés d'investir dans des mesures qui ont été testées, qui ont donné des résultats positifs et qui de plus sont recommandées par des criminologues ou d'autres personnes ayant une expertise en sécurité.

L'étude 'Hakim-Buck study on suburban alarm effectiveness'[5] a été citée par Cynthia dans l'un de ses rapports. Simon Hakim et Andrew J. Buck sont deux professeurs en économie s'étant intéressés à la question des introductions par effraction. Cynthia cite cette étude pour justifier l'installation d'un détecteur de bris de verres qui est dispendieux. Elle mentionne dans son rapport que cette étude démontre que 79 % des voleurs s'introduisent par effraction par le sous-sol ou par l'un des points d'entrées du rez-de-chaussée. Elle connaît donc l'importance de mieux protéger les fenêtres et les portes donnant sur ces deux niveaux des établissements.

4.15 Les experts, la littérature spécialisée et les concepts criminologiques

Tel que nous l'avons démontré dans ce mémoire, pratiquement tous les experts rencontrés utilisent une petite ou une grande partie de la littérature présentée dans la recension des écrits. Si la ressemblance entre la littérature spécialisée et la façon de faire des experts rencontrés était frappante, il en est autrement pour les théories et les concepts proposés par les criminologues. Les professionnels connaissent et se réfèrent souvent aux ouvrages traitant de la sécurité privée. Ils affectionnent particulièrement les ouvrages dans lesquels nous y trouvons des exemples de guides de sécurité. Beaucoup ont mentionné s'être inspirés de cette littérature pour développer leurs

[5] Hakim, S. et Buck, A.-J. (1991) *Hakim-Buck study on suburban alarm effectiveness*, Philadelphia

méthodes de travail et pour construire les guides utilisés pour inspecter les organisations. Contrairement à ces ouvrages, les experts ont beaucoup moins mentionné les concepts et les théories développés par les criminologues. Six experts sur seize nous ont parlé de concepts élaborés en criminologie et cette question a toujours occupé une petite place dans l'interview. Cinq de ces experts avaient un lien avec l'école de criminologie (professeurs ou diplômés).

5. CAS ENTREPÔT FROST (OBSERVATION)

Dans le cadre de notre cueillette des données, deux séances d'observation ont été effectuées. L'une d'elles s'est déroulée à l'entrepôt Frost. Nous avons alors accompagné deux experts qui en étaient à leur deuxième visite chez ce client. La séance a duré une après-midi. Dans un premier temps, le demandeur a été rencontré et plusieurs questions lui ont été posées. Dans un deuxième temps, nous avons visité les lieux en compagnie du demandeur. Nous n'avons pas apporté de contribution au projet. Nous accompagnions les deux experts et observions l'interaction qu'ils avaient avec le demandeur et les employés. Nous observions aussi le travail qu'ils effectuaient sur le terrain. Un exemplaire du rapport nous a été remis. Ce chapitre est important dans la mesure où nous donnons un exemple concret d'audit.

5.1 Présentation des experts

Les experts travaillent à temps plein pour deux organisations différentes et offrent aussi des services-conseils pour d'autres entreprises. James a 24 ans d'expérience dans le domaine de la sécurité. Il est membre de l'ASIS International et détient la formation CPP. Il a des connaissances approfondies au sujet de l'audit de sécurité et de l'analyse de risques. De son côté, Myriam possède 18 ans d'expérience en sécurité. Elle accompagnait James pour l'aider à recueillir les informations sur le terrain, à questionner les employés, à observer les lieux, à rechercher des informations clés dans la littérature et à rédiger le rapport final.

5.2 Entrepôt Frost

L'entreprise où l'audit s'est déroulé se spécialise dans l'entreposage de produits finis. Il s'agit de l'un des nombreux sites d'une entreprise établie depuis une soixantaine d'années et qui œuvre à l'international. Le nom Frost est fictif et a été donné pour une question d'anonymat. Cet entrepôt se situe dans un quartier industriel de la ville de Montréal et sa capacité de stockage est importante. Il y a au plus une cinquantaine

d'employés qui travaillent sur ce site. Cet entrepôt semble être actif pour l'entreprise Frost depuis une quinzaine d'années. Il y avait déjà des systèmes et des procédures de sécurité en place.

Mark est le gestionnaire principal du site et la personne responsable du projet. Il est le directeur général de la division du Québec pour l'entreprise et compte une vingtaine d'années d'ancienneté. Il a une excellente connaissance de son site et maîtrise les systèmes de sécurité en place. Le mandat a été négocié avec ce gestionnaire. Notre rencontre s'est déroulée avec lui et il nous a accompagné sur le terrain pour visiter les lieux. Le rapport lui a été présenté en plus d'avoir été exposé au Comité directeur qui s'occupe de la sûreté.

La principale raison expliquant la demande de l'audit est la volonté de vérifier si l'entrepôt se conforme au programme 'Customs-Trade Partnership Against Terrorism' (C-TPAT). Il semble que Mark savait dès le départ qu'il y aurait des modifications à apporter pour obtenir cette accréditation et il voulait obtenir l'opinion d'experts pour voir les aspects qui n'étaient pas conformes aux différentes exigences. Il a aussi profité de la présence des experts pour élargir le mandat et faire vérifier la sécurité sur l'ensemble du site. De plus, Mark voulait obtenir une vue d'ensemble du niveau de sécurité de son site et en connaître les vulnérabilités ainsi que les forces. Il souhaitait obtenir des recommandations dans le but de sécuriser le site, c'est-à-dire de protéger les employés, les actifs, ses informations et la réputation de l'entreprise.

Lors de la rencontre qui s'est déroulée avec Mark, nous avons constaté que des systèmes de sécurité venaient d'être installés sur le site. Au moment où l'audit débutait, des budgets étaient déjà à l'étude pour installer d'autres équipements de sécurité. Il nous semble étrange que des demandes soient déjà faites avant même que l'entreprise soit auditée. Quel est l'intérêt pour un gestionnaire d'installer des systèmes et de faire la demande pour de nouveaux équipements avant même d'avoir les résultats de l'audit ? Il nous semble préférable d'attendre les résultats avant de faire des demandes à ce sujet. Ce qui est remarquable, c'est que Mark semblait déjà regretter

des choix vis-à-vis le système de caméras qu'il avait fait mettre en place. Dans le rapport, James et Myriam critiquent quelques mesures demandées par Mark. L'implantation de certaines d'entre elles est retardée tandis que d'autres se doivent d'être modifiées pour donner l'effet désiré.

5.3 Travail effectué par les experts

L'ensemble du projet est constitué de quatre visites sur les lieux et de la rédaction d'un rapport qui a été présenté au demandeur ainsi qu'au Comité directeur.

5.3.1 Première visite

La première visite fut organisée pour rencontrer Mark. Elle avait pour but de négocier le mandat et de connaître ses attentes. Les experts lui ont aussi demandé de préparer des outils de travail pour faciliter les visites ultérieures (exemple : plan des lieux). Une courte inspection eut lieu pour prendre connaissance du site. Des vulnérabilités ont été constatées dès la première tournée des lieux. Ces constats se retrouvent d'ailleurs dans le rapport final. Des photos ont été prises.

5.3.2 Deuxième visite

Notre séance d'observation s'est déroulée lors de cette deuxième rencontre entre le demandeur et les experts. Cette visite peut être divisée en deux parties. La première partie étant la rencontre avec Mark et la deuxième étant l'inspection du site.

La rencontre avec Mark fut d'une durée approximative d'une heure. James a posé les questions qu'il avait préparées dans son guide de sécurité. Plusieurs questions ont été posées au sujet de l'entreprise, du site, des employés, des actifs, des vulnérabilités connues du demandeur et des autres personnes en mesure d'aider les experts dans leur recherche d'informations. Le guide a été rempli en partie à l'aide des informations données par Mark. Il n'avait pas toujours les réponses aux questions. Dans ce cas, il

donnait le nom des personnes en mesure d'y répondre. Mark a une bonne connaissance de son entreprise et a su informer les experts sur différents sujets. Il connaît plusieurs vulnérabilités ou endroits chauds où il est possible de trouver des problèmes. Il est conscient du fait qu'il dispose une quantité importante d'ammoniaque susceptible d'affecter l'entreprise et même d'avoir un impact majeur sur un rayon important dans le cas où il y aurait une fuite accidentelle ou intentionnelle. Une discussion a aussi porté sur les différentes procédures mises en place dans l'entreprise pour éviter des problèmes. Par exemple, une politique en place empêche les employés d'acheter des produits endommagés. Cela évite qu'ils abîment intentionnellement les produits pour les acheter à rabais. De plus, un système de collecte des ordures est conçu de façon à empêcher les employés de jeter des produits qui pourraient par la suite être ramassés. Une autre politique permet aux femmes de stationner leur voiture près de la porte d'entrée durant la nuit. Elles se sentent davantage en sécurité et cela évite qu'elles aient à marcher sur une longue distance pour accéder à leur véhicule. Bref, les experts posent les questions qu'ils jugent pertinentes et Mark les informe des points susceptibles de les aider.

Après la rencontre, une visite en compagnie de Mark eue lieu. Elle fut d'une durée approximative de deux heures. Mark était à nos côtés pour nous diriger sur le site et surtout pour répondre aux différentes questions des experts. Des photos ont été prises et quelques employés ont rapidement été rencontrés. Nous avons regardé le fonctionnement du système de surveillance électronique et visionné le moniteur dans le bureau du demandeur.

Avant de quitter, James a demandé à ce que les employés soient mis au courant qu'un audit était en cours sur le site. Il a demandé une carte d'accès pour les visites éventuelles, ce à quoi Mark a acquiescé.

En quittant les lieux, un employé nous invite à entrer dans une zone contrôlée et cela sans être accompagné par un responsable. Il s'agit d'une vulnérabilité qui a été immédiatement perçue et notée par les experts. À tout moment, des incidents de ce

genre peuvent se produire sur le terrain. L'expert doit être vif d'esprit et les noter. Pour certains, cet incident aurait pu paraître anodin, alors qu'en réalité il s'agit d'une faiblesse sur le plan des contrôles d'accès. À quoi bon investir dans un système de cartes d'accès si les employés se font le plaisir d'ouvrir les portes aux gens de l'extérieur ?

5.3.3 Autres visites

Suite à la visite à laquelle nous avons assistée, deux autres visites se sont déroulées. Les experts ont alors examiné les lieux en détail. Ils ont rencontré certaines personnes qui étaient en mesure de les renseigner sur l'organisation et ses problèmes. Ils ont consulté différents documents comme les politiques et les procédures de l'entreprise ainsi que les contrats d'assurance.

5.3.4 Rapport

Le rapport est constitué de 46 pages. Il s'agit d'un document bien aéré et rédigé à interligne simple. La présentation est soignée. Le rapport est séparé en différentes sections : la page de présentation, la table des matières détaillée, l'introduction, le sommaire exécutif et la partie centrale du rapport qui consiste à rapporter les constats et les recommandations. Pour terminer, une petite section à la fin indique si l'entreprise se conforme ou non aux exigences C-TPAT.

Les constats et les recommandations sont séparés en catégories. Tout ce qui se rapporte au périmètre est discuté dans une section. Ce qui a trait à l'entrepôt est discuté dans une autre section, et ainsi de suite. Cette séparation est faite en fonction d'un lieu, d'un système ou d'un genre d'évènement. Les recommandations sont mises dans leur contexte et précédées des constats. James et Myriam trouvent qu'il s'agit d'une bonne façon de présenter ces informations. Cynthia partage cet avis. En présentant le rapport de cette manière, il est plus facile pour les lecteurs d'associer les constats avec leurs

recommandations. Il est plus difficile de faire ces liens si les constats sont tous dans un même bloc et que les recommandations se trouvent dans une autre section.

Plusieurs informations sont présentées dans la section 'contexte' qui précède les constats. Voici des informations que nous retrouvons dans cette partie :

1) Des 'bonnes façons de faire' sont présentées. Celles-ci sont choisies en fonction des constats et des recommandations qui les suivent. Les experts indiquent par exemple des mesures qui sont utilisées et qui donnent normalement de bons résultats.
2) Les responsabilités de la compagnie sont exposées.
3) Des cas documentés sont présentés. Les experts donnent l'exemple d'un feu qui a détruit le site d'une compagnie qui se disait bien protégée contre les incendies et font un parallèle avec l'entrepôt Frost. Les employés de l'entrepôt ont développé un faux sentiment de sécurité en se fiant énormément sur le système de gicleurs en place. James et Myriam sont d'accord pour dire qu'il s'agit d'un bon système, mais mentionne que d'autres actions doivent être prises pour éviter les feux. Une 'brigade incendie' formée d'employés aide à prévenir les dommages reliés à un feu.
4) Des concepts théoriques sont exposés. Par exemple, les experts expliquent qu'un vol survient s'il y a la présence de trois éléments soit, l'opportunité, la rationalisation et la motivation. À un autre endroit, ils expliquent le concept des quatre 'D' pour se protéger contre les vols qui sont : detect, deter, delay et deny. Les définitions des mots 'risque' ou 'contrôle des risques' sont données. Ils expliquent aussi la notion de 'crise' et mentionnent que ce terme est souvent incompris et utilisé d'une façon inadéquate.
5) Des exemples de 'modus operandi' sont donnés pour expliquer au client comment des voleurs pourraient s'en prendre aux actifs sur le site.
6) Des précisions sont données sur la façon d'utiliser certains systèmes de sécurité. Par exemple, ils exposent les conditions qui font qu'un système de surveillance donnera de bons résultats ou pas (bonne qualité d'image, possibilité de rapprochement, visionnement en temps réel et intervention rapide).
7) Les avantages de certains systèmes sont énumérés et les coûts qui y sont rattachés sont mentionnés.

8) Les raisons pour lesquelles certaines situations peuvent créer des problèmes ou des vulnérabilités pour l'entreprise sont expliquées. Prenons l'exemple du niveau d'éclairage sur le périmètre. Un système d'éclairage bien pensé et bien entretenu diminue les chances d'être victime d'un crime et les experts expliquent pourquoi. À l'inverse, un site mal éclairé permet aux gens de circuler sans être perçu.

Plusieurs informations et explications se trouvant dans la section 'contexte' aident le lecteur à mieux comprendre les constats et les recommandations qui suivent.

Par la suite, les constats qui ont été faits sur le terrain sont présentés. Les observations, les discussions et les lectures sont rapportées. Les experts ne se limitent pas seulement aux lacunes perçues. Ils mettent aussi l'accent sur les éléments forts qui doivent être maintenus en place pour conserver un niveau de sécurité acceptable.

Dans un troisième temps, des mesures sont recommandées pour régler les problèmes. Essentiellement, les recommandations sont constituées de procédures, de systèmes, de technologies ou du maintien en place de mesures déjà existantes.

Le contexte, les constats et les recommandations sont donc présentés au lecteur en trois temps et séparés en catégories. Normalement, chaque bloc est d'une longueur qui varie entre une et trois pages. Il est donc facile d'associer les recommandations avec le contexte et les constats qui s'y rattachent.

5.4 Présentation du rapport et fin du projet

Le rapport a été présenté au Comité de direction composé de membres de différents niveaux décisionnels (des gestionnaires et des gens affectés aux opérations). La présentation a été appuyée d'un document PDF et d'un diaporama. L'entrepôt ayant été vendu par la suite, les experts ne savent pas ce qui est advenu des recommandations.

CONCLUSION

La plupart des gestionnaires sont appelés à s'interroger sur la sécurité de leur organisation : est-elle adéquate ? Idéalement, les décideurs implantent des mesures de sécurité avant que les problèmes affectent leur organisation. Toutefois, il n'est pas toujours facile pour eux d'évaluer la sécurité et de percevoir leurs forces ainsi que leurs faiblesses. La difficulté augmente en fonction du degré de négligence qu'il y a eu à cet égard au fil du temps. Il est difficile de construire un programme de sécurité pour un nouveau site ou pour une nouvelle organisation. Les choix qu'ils doivent faire dans ce domaine ne sont pas évidents puisqu'il y a une panoplie grandissante de ressources offertes pour atteindre un niveau de sécurité acceptable. Agencer ces ressources de façon cohérente et efficace nécessite parfois l'aide de gens ayant une expertise dans ce domaine.

Certaines organisations ont les moyens d'engager des spécialistes qui travaillent pour elles à temps plein et qui s'occupent de ces questions. D'autres entreprises comptent sur l'aide sporadique de spécialistes qu'elles appellent pour exécuter des contrats. Au Québec, des gens offrent différents produits et services pour améliorer la sécurité des organisations. Certains travaillent pour des entreprises qui offrent à la fois des services-conseils et différents produits. D'autres se spécialisent dans l'un ou l'autre de ces secteurs du marché. Quand vient le temps d'investir en sécurité, il est important de faire appel à des gens capables d'identifier les besoins et de trouver des mesures qui y sont adaptées. Il faut se méfier des experts qui recommandent des mesures pour leur propre intérêt et non pour celui de l'organisation qui est de se protéger adéquatement. Les mesures dans lesquelles elles investissent doivent prévenir les problèmes ou les corriger efficacement.

Il n'est pas rare de voir des professionnels recommander des solutions sans avoir au préalable fait une analyse sérieuse de la situation. L'audit de sécurité est un outil intéressant qui aide à effectuer cette analyse et à évaluer les besoins réels d'une organisation. En auditant un site, l'expert rencontre des gens, fait différentes

observations, prend des clichés des lieux et lit des documents. Ce travail sur le terrain lui permet de recueillir une somme d'informations et de données qui lui permettent d'identifier les risques encourus par l'organisation, de relever les faiblesses ainsi que les forces du système de protection en place et finalement de statuer sur le niveau de sécurité. Grâce à cette démarche, il lui est plus facile de recommander des solutions efficaces aux problèmes identifiés. Sans faire de cueillette et d'analyse des données, sans connaître la mission, les priorités organisationnelles, le plan d'affaires et les opérations de l'organisation, il semble difficile d'identifier les problèmes sécuritaires et de recommander des mesures permettant de les régler.

Pour la majorité des experts rencontrés, il ne s'agit pas d'un projet qui s'improvise. Ils sont conscients de l'importance de procéder par étapes et de ne pas arriver aux solutions trop rapidement. Le projet est souvent constitué de cinq étapes. 1) Une visite préliminaire est organisée pour rencontrer le demandeur du projet dans le but de négocier un mandat clair avec lui. Une visite sommaire des lieux est normalement effectuée à cette étape pour observer rapidement les installations et se donner une idée du projet qui s'annonce. 2) L'expert prépare le projet. Il organise ses idées, planifie les actions futures, assemble les outils qui lui seront nécessaires et développe un guide de sécurité adapté à l'organisation. Il fait aussi appel à des collaborateurs si c'est nécessaire. 3) Il se rend sur le site pour recueillir les informations et les données. 4) Il analyse les données. 5) Il trouve des solutions aux problèmes, fait ses recommandations et rédige un rapport qui sera donné et présenté au demandeur ainsi qu'aux gestionnaires.

Les experts et les demandeurs doivent travailler avec des contraintes qui affectent la qualité de leur travail. Les principales contraintes sont le manque d'argent et de temps. D'autres organisations doivent négocier avec des employés qui sont fermés aux changements qui ont trait à la sécurité. En effet, certains s'opposent vigoureusement aux systèmes et aux procédures qui sont mis en place dans les organisations. Il est dans l'intérêt de tous de considérer ces contraintes et de voir à ce qu'elles affectent le moins possible la qualité des audits et l'implantation des mesures qui suivront le projet.

Aux États-Unis, l'audit a largement été documenté par des auteurs détenant une expertise en sécurité des organisations. Tout au long de notre recherche, nous avons constaté que la majorité des experts rencontrés connaissent cette littérature et l'utilisent. Il s'agit principalement de personnes ayant un lien avec l'organisation ASIS International. Cette organisation, appuyée par son chapitre à Montréal, rend disponibles plusieurs ressources qui aident les professionnels à maintenir leurs connaissances à jour. Il y a des experts à Montréal qui sont familiers avec l'audit de sécurité et qui en réalisent pour leurs clients ou pour les organisations qui les embauchent. Parmi eux, certains ont insisté sur l'importance de faire un travail consciencieux, professionnel et rigoureux.

En examinant correctement l'entreprise, il est plus facile de trouver les problèmes et de les résoudre en utilisant des mesures qui s'intègrent aisément aux dispositifs déjà en place. Selon James et Sylvio, l'audit devrait être perçu comme le pilier de la sécurité d'une organisation. Aucun programme de sécurité ne devrait être développé sans qu'un relevé soit fait au préalable. Celui-ci permet d'avoir une bonne vision d'ensemble des installations. Ainsi, il est possible de visualiser les endroits où il est pertinent d'ajouter des mesures de sécurité tout en les intégrant aux autres déjà en place et en évitant d'installer des systèmes redondants. De plus, le relevé permet d'investir intelligemment, c'est-à-dire de protéger adéquatement l'organisation tout en réduisant au maximum les dépenses. Ils ont vivement critiqué ceux qui n'ont pas de méthode et qui recommandent des mesures sans avoir minimalement analysé l'organisation.

Dans cette recherche, nous avons constaté que la majorité des experts rencontrés connaissent et utilisent la littérature spécialisée pour réaliser leurs audits de sécurité ainsi que pour développer leurs guides de sécurité. Il y en a moins qui s'inspirent des concepts criminologiques dans le cadre de leur travail. Ces ouvrages rédigés par les criminologues sont moins connus, maîtrisés ou utilisés. Nous voulons mettre l'emphase sur deux points. Le premier est d'établir une jonction entre le savoir-faire qui a été développé par les experts de la sécurité et celui des criminologues. Le

deuxième apport serait d'exploiter davantage les données quantitatives et les statistiques.

En jumelant l'expertise des spécialistes de la sécurité et le savoir-faire des criminologues qui se sont intéressés à la prévention du crime, à la dissuasion, à la prévention situationnelle ainsi qu'à la résolution de problèmes, l'auditeur n'est que mieux outillé pour inspecter une organisation. En utilisant davantage cette expertise et les forces de chacun, il en résulterait une meilleure cueillette des données et une analyse plus juste. La force du 'security survey' tel que développé par les professionnels de la sécurité privée et par les membres de l'ASIS International est de présenter des implications pratiques immédiates et souvent évidentes. Cette façon pragmatique de faire la sécurité n'est pas maîtrisée parfaitement par les criminologues et ils ont à apprendre de cette méthode. Par contre, la faiblesse de cette façon de faire est de négliger l'analyse des données sur les incidents passés et sur les infractions qui ont déjà été commises. Cela a comme résultat qu'il est plus difficile de détecter, de comprendre et de contrer les pratiques criminelles émergentes. À ce niveau, les criminologues réussissent mieux que les professionnels de la sécurité privée. En opérant la jonction entre l'analyse proposée par les criminologues et les recommandations pratiques des experts de la sécurité privée, l'audit n'en serait qu'amélioré.

Deux grandes catégories de données peuvent être amassées durant un audit, soit les données quantitatives et qualitatives. Nous avons constaté que les données recueillies sur le terrain sont principalement qualitatives. Essentiellement, elles se limitent aux informations obtenues lors des rencontres avec les employés, pendant les séances d'observation et par la lecture de différents documents. L'expert se doit de faire ce travail sur le terrain pour rencontrer les gens, observer les lieux et lire les documents. Toutefois, il serait avantageux d'utiliser davantage les données quantitatives. Quelques experts ont souligné la difficulté de recueillir des statistiques ou des rapports d'incidents puisque ce ne sont pas toutes les organisations qui les compilent. Par ailleurs, certaines organisations amassent ces informations d'une façon peu organisée

et non rigoureuse de sorte qu'il est impossible de les utiliser pour en faire des analyses intéressantes. Éventuellement, nous croyons que les données quantitatives seront plus faciles à obtenir et pourront être mises à la disposition des experts ayant à réaliser des audits de sécurité. Des applications informatiques accessibles et faciles à utiliser sont offertes sur le marché. Elles permettent de compiler les informations intelligemment, ce qui les rend plus faciles à obtenir et à utiliser. En combinant les données qualitatives et quantitatives, il en résulterait une meilleure analyse et une compréhension accrue des problèmes. De plus, il serait plus aisé de vérifier si les recommandations mises en place suite au projet donnent des résultats significatifs. À l'aide des statistiques, il est possible de comparer la période qui précède la mise en place de mesures de sécurité avec la période qui suit afin de vérifier s'il y a une diminution du nombre d'incidents. À ce sujet, nous invitons le lecteur à consulter la recension des écrits du présent mémoire et à utiliser la technique d'évaluation proposée par Cusson et coll. (1994 : 40-41).

En guise d'ouverture, nous croyons qu'une recherche éventuelle pourrait porter sur les résultats qui sont obtenus suite à la réalisation des audits de sécurité. Il serait pertinent de vérifier si les programmes de sécurité qui ont été précédés d'un audit de sécurité sont mieux construits et plus efficaces que les programmes qui ont été faits sans cette analyse. Est-ce que les organisations qui sont auditées périodiquement ont de meilleurs résultats en ce qui a trait à la sécurité ?

Bibliographie

AQIS (2004) *Livre blanc: la sécurité privée – partenaire de la sécurité intérieure*, Mémoire présenté à la Commission des institutions de l'Assemblée nationale

ASIS International (2001) *Physical Security*, Washington, ASIS International

ASIS International (2003) *General Security Risk Assessment: An ASIS International Guideline*, Alexandria, ASIS International

ASIS International (2004) *Chief Security Officer (CSO) Guideline*, Alexandria, ASIS International

Bacher, J-L, Gagnon, C. (2003) *Traité de la criminologie empirique; troisième édition* Montréal, Les presses de l'Université de Montréal, pp. 73-110.

Bacher, J-L., Cousineau, M.-M. (1999) *Heurts et bonheurs à l'heure de la collaboration entre enquêteurs privés et policiers* in Shapland, L. Van Outrive (Eds) Police et sécurité : contrôle social et interaction public/privé. Paris, 101-114

Biegaj, K. (2000) *Services de sécurité interne : mise en parallèle de modes de fonctionnement.* Mémoire de maîtrise, École de criminologie, Université de Montréal

Blais, M-F (1999) *Le secteur de l'enquête privée au Québec : implications pour le contrôle social et démocratique.* Mémoire de maîtrise, École de criminologie, Université de Montréal

Broder, J. F. (2000) *Risk Analysis and the Security Survey* 2nd edition. Boston Butterworth-Heinemann

Broder, J. F. (2006) *Risk Analysis and the Security Survey* 3nd edition. Boston Butterworth-Heinemann

Brodeur, J.-P. (1995) *Le contrôle social : privatisation et technocratie* Déviance et Société, Vol. 19, No 2, pp. 127-147.

Brodeur, J.-P. (2003) *Les visages de la police : pratiques et perceptions* Montréal Les presses de l'Université de Montréal pp. 283-339.

Clarke R. V. et Eck, J. (2003) *Become a Problem Solving Crime Analyst : in 55 Small Steps* London, Jill Dando Institute of crime science, University College London

Commission du droit du Canada (2002) *En quête de sécurité : le rôle des forces policières et des agences privées*

Collins, P. A., Ricks, T. A., et Van Meter, C. W. (2000) *Principles of Security and Crime Prevention, Fourth Edition* Cincinnati, Anderson Publishing co.

Cornish, D. B. et Clarke, R. V. (1986) *The Reasoning Criminal: Rational Choice Perspective on Offending* New York, Springer-Verlag

Cunningham, W. C., Strauchs, J. J. Et Van Meter, C. W. (1990) *Private Security Trends, 1970 to 2000: The Hallcrest Report II*, Toronto, Butterworth-Heinemann.

Cusson, M. (1981) *Délinquants pourquoi ?* Montréal, Hurtubise HMH

Cusson, M. (1993) *L'effet structurant du contrôle social* Revue Criminologie, XXVI, 2, 37-62

Cusson, M. (1994) *La sécurité privée, sa nature, sa raison d'être et son avenir* Montréal, Les cahiers de l'École de criminologie

Cusson, M., Tremblay, P., Biron, L. L., Ouimet, M. et Grandmaison, R. (1994) *La planification et l'évaluation des projets en prévention du crime* Recherche commandée par le Ministère de la Sécurité publique du Québec

Cusson, M. (1998) *La sécurité privée : le phénomène, la controverse, l'avenir.* Revue Criminologie, XXXI, no 2, p. 31 à 46

Cusson, M. (2000) *La criminologie* 3e édition. Paris. Hachette

Cusson, M. (2002) *Prévenir la délinquance : les méthodes efficaces* Paris : Presses universitaires de France

Cusson, M. (2005) *La délinquance, une vie choisie.* Montréal : Éditions Hurtubise HMH ltée

Cusson, M. (2007) *La prévention : les principes et la prévention policière*, Traité de sécurité intérieure, chapitre 27

Cusson, M. (2007) *Comment prévenir ? Les techniques et la méthode de la prévention situationnelle*, Traité de sécurité intérieure, chapitre 28

Cusson, M. (2007) *La surveillance et la contre-surveillance*, Traité de sécurité intérieure, chapitre 29

Cusson, M. (2007) *La télésurveillance*, Traité de sécurité intérieure, chapitre 31

Dégailler, F. (1997) *Étude de marché des agences de sécurité à contrat à Montréal et au Québec* Mémoire de maîtrise, École de criminologie, Université de Montréal

Dégailler, F. (1998) *Sécurité privée au Québec, un marché en évolution ?* Revue Criminologie, XXXI, no. 2, 47-67

Deslauriers, J.-P., Kérisit, M. (1997) *Le devis de recherche qualitative*, in J. Poupart, J.-P. Deslauriers, L. Groulx, A. Laperrière, R. Mayer, A. Pires (Eds) : La recherche qualitative : enjeux épistémologiques et méthodologiques, Boucherville, Gaëtan Morin, 85-111

Diaz, F. (2005) *L'observation participante comme outil de compréhension du champ de la sécurité* Champ pénal : Nouvelle revue française de criminologie, vol II.

Felson, M. (2002) *Crime and Everyday life third edition* Thousand oaks, Sage publications

Felson, M. et Clarke, R. V. (1998) *Opportunity Makes the Thief : Practical Theory for Crime Prevention.* Policing & Reducing Crime, Police Research Series, Paper 98

Fennelly, L. J. (2004 a) *Effective Physical Security 3rd Edition.* Burlington, Elsevier Butterworth-Heinemann

Fennelly, L. J. (2004) *Handbook of Loss Prevention and Crime Prevention 4nd Edition.* Amsterdam, Elsevier Butterworth-Heinemann

Fisher, J. R., Green, G. (2004) *Introduction to Security 7nd Edition.* Boston Butterworth-Heinemann

Foucaudot, M. (1988) *Étude descriptive sur les agences de sécurité privées au Québec* Mémoire de maîtrise, École de criminologie, Université de Montréal

Gagnon, P. (2006) *L'audit sécurité* Paris, Afnor

Garcia, M. L. (2001) *The Design and Evaluation of Physical Protection Systems*, Woburn: Butterworth-Heinemann

Garcia, M. L. (2006) *Vulnerability Assessment of Physical Protection Systems*, Burlington, Elsevier Butterworth-Heinemann

Geiben, B., Nasset, J.-J. (1998) *Sécurité sûreté : la gestion intégrée des risques dans les organisations*, Paris, Les Éditions d'Organisation

Gendarmerie royale du Canada (2000) *Guide de sécurité (SST/GS-25) : guide pour la préparation d'un énoncé de sécurité matérielle*

Grose, V. L. (1987) *Managing Risk: Systematic Loss Prevention for Executives*, New Jersey, Prentice Hall

Hess, M. K., Wrobleski, H. M. (1992) *Introduction to Private Security, Third edition*, St-Paul, West publishing company

IHESI (1991) *Le marché de la sécurité privée* Les cahiers de la sécurité intérieure, no. 3, novembre 1990 – janvier 1991

Killias, M. (1991) *Précis de criminologie*, Berne, Staemplfi

Kingsbury, A. A. (1973) *Introduction to Security and Crime Prevention Surveys*, Springfield, Charles C Thomas publisher

Le Doussal, R. (1991) *La sécurité privée dans un service public: un an d'expérience à l'assistance publique*, Les cahiers de la sécurité intérieure, no 3, 113-130

Le Doussal, R. et Laures-Colonna, P. (1992) *La sécurité à l'hôpital*, Paris, Éditions ESF.

Le Doussal, R. (1995 a) *À l'hôpital : anti-malveillance et technologie*, Les cahiers de la sécurité intérieure, no 21, 75-87

Le Doussal, R. (1995 b) *La lutte contre les vols*, Gestions hospitalières, oct 1995, 595-601

Leman-Langlois, S. (2007) *L'analyse de problèmes de sécurité et la conception de solutions adaptées*, Traité de sécurité intérieure, chapitre 25

Leman-Langlois, S. et Dupuis, L. (2007) *Les technologies de protection des espaces*, Traité de sécurité intérieure, chapitre 30

Michelat, G. (1975) *Sur l'utilisation de l'entretien non directif en sociologie*, Revue française de sociologie, XVI, 229-247

Mignault, S. (2007) *L'audit de sécurité et la protection des organisations*, Traité de sécurité intérieure, chapitre 26

Ministère de la sécurité publique (2003) *Livre blanc : la sécurité privée - partenaire de la sécurité intérieure*

Momboisse, R. M. (1968) *Industrial Security for Strikes, Riots and Disasters*, Springfield, Charles C Thomas publisher

National Crime Prevention Institute (1986) *Understanding crime prevention*, Stoneham Butterworths

Ocqueteau, F. (1991) Les marchés de la sécurité privée : développement et implications In. IHESI (Eds) *Le marché de la sécurité privée*, Les cahiers de la sécurité intérieure, no. 3, novembre 1990 – janvier 1991, 81-111

Paillé, P. (1994) *L'analyse par théorisation ancrée* Cahiers de recherche sociologique, 23, 147-181

Paillé, P. (1996) *Qualitative par théorisation ancrée (analyse de contenu)* in A. Mucchielli (ed.) : Dictionnaire des méthodes qualitatives en sciences humaines et sociales, 184-190, Paris : Armand Collin

Peretz, H. (1998) *Les méthodes en sociologie : l'observation* Paris, Éditions La Découverte

Piché, D. (2000) *Les relations de coopération entre la police et le secteur de l'investigation privée au Québec : la perspective de l'enquêteur de police.* Mémoire de maîtrise, École de criminologie, Université de Montréal

Pires, A. P. (1997) *Échantillonage et recherche qualitative : essai théorique et méthodologique*, in J. Poupart, J.-P. Deslauriers, L. Groulx, A. Laperrière, R. Mayer, A. Pires (Eds) : La recherche qualitative : enjeux épistémologiques et méthodologiques, Boucherville, Gaëtan Morin, 113-169

Poupart, J. (1997) *L'entretien de type qualitatif : considérations épistémologiques, théoriques et méthodologiques*, in J. Poupart, J.-P. Deslauriers, L. Groulx, A. Laperrière, R. Mayer, A. Pires (Eds) : La recherche qualitative : enjeux épistémologiques et méthodologiques, Boucherville, Gaëtan Morin, 173-209

Purpura, P. P. (2002) *Security and Loss Prevention Introduction 4nd Edition.* Boston Butterworth-Heinemann

Rengert, G. F., Mattson, M. T. Et Henderson, K. D. (2001) *Campus Security Situational Crime Prevention in High-Density Environments.* Monsey, Criminal Justice Press

Roux-Dufort, C. (2003) *Gérer et decider en situation de crise*, DUNOD, Paris

Roper, C. A. (1999) *Risk Management for Security Professionnals* Boston, Elsevier, Butterworth-Heinemann

Schaub, J. L, Biery, K. D. (1998) *The Ultimate Security Survey 2nd edition.* Boston Butterworth-Heinemann

Sennewald, C. (2003) *Effective Security Management 4nd Edition.* Boston Butterworth-Heinemann

Service de police de la Ville de Montréal, *Vos biens sont-ils en sécurité*, dépliant offerts aux citoyens pour les aider à protéger leurs biens

Service de police d'Ottawa (2003) *Programme inspection à domicile : liste de contrôle* Programme de prévention mis en place pour les citoyens

Shearing, C. D. et Stenning, P. C. (1985) *Sécurité privée* Journal du Collège canadien de police, Vol. 9, No. 4, pp. 401-424

Shearing, C. D. « Punishment and the Changing Face of Governance », *Punishment and Society*, 3, 2, 2000, p. 203-220

Tesch, R. (1990) *Qualitative Research : Analysis Types and Software Tools* Bristol, Pa.: Falmer Press

Tucker, E. (2000) Crime Prediction. In J. F. Broder (Ed.) *Risk Analysis and the Security Survey* 2nd edition. Boston: Butterworth-Heinemann

Tyska, L. A et Fennely, L. J. (1998) *150 Things you Should Know About Security* Boston Butterworth-Heinemann

Université de Montréal (2004) *Document de réflexion sur le livre blanc : la sécurité privée - partenaire de la sécurité intérieure*, Document présenté au Ministère de la Sécurité publique du Québec

Walsh, T. J. and Healy, R. J. (1994) *Protection of Assets (POA)*. Santa Monica, ASIS International